HP ProtectTools セキュリティ ソフトウェア バージョン 6.0

ユーザー ガイド

HP ProtectTools セキュリティ ソフトウェア ユーザー ガイド

改訂第 2 版：2010 年 11 月

製品番号：581746-293

このガイドについて

このガイドでは、このコンピューターの機能およびハードウェアのアップグレードについて説明します。

⚠ **警告！** その指示に従わないと、人体への傷害や生命の危険を引き起こすおそれがあるという警告事項を表します。

△ **注意：** その指示に従わないと、装置の損傷やデータの損失を引き起こすおそれがあるという注意事項を表します。

注記： 重要な補足情報です。

目次

1 セキュリティの概要

HP ProtectTools セキュリティ ソフトウェアは、コンピューター本体、ネットワーク、および重要なデータを不正なアクセスから保護するために役立つセキュリティ機能を提供します 。 複 数 の HP ProtectTools ソフトウェア モジュールによって、高度なセキュリティ機能が提供されます。

[HP ProtectTools]では、2 つのバージョンを利用できます。HP ProtectTools Security Manager 管理者コンソールおよび HP ProtectTools Security Manager（一般ユーザー用）です。管理者用バージョンもユーザー用バージョンも、**[スタート]**→**[すべてのプログラム]**→**[HP]** メニューから利用できます。

バージョン	機能
HP ProtectTools Security Manager 管理者コンソール	• アクセスするには、Microsoft® Windows®システム管理者のアクセス権が必要です • 各モジュールへのアクセスは管理者が設定するものであるため、一般ユーザーは使用できません • すべてのユーザー用の初期セキュリティを設定したり、オプションや必須要件を構成したりできます
HP ProtectTools Security Manager（一般ユーザー用）	• 管理者によって提供されたオプションをユーザーが構成できます • アクセスを制限して、一部の HP ProtectTools モジュールの限られた調整機能しかユーザーが使用できないようにすることができます

注記： パスワード マネージャー、Smart Card Security、Face Recognition（一部のモデルのみ）、および Drive Encryption は、Security Manager セットアップ ウィザードを使用して設定します。HP Professional Desktop システムでは現在、指紋認証デバイスがサポートされていません。

HP ProtectTools ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、設定可能なオプションまたは製品購入後のオプションとして導入できる場合があります。詳しくは、http://www.hp.com/jp/を参照してください。

注記： このガイドの操作手順は、該当する HP ProtectTools ソフトウェア モジュールがすでにインストールされていることを前提に記述されています。

HP ProtectTools の機能

以下の表で、HP ProtectTools モジュールの主な機能を詳しく説明します。

モジュール	主な機能
HP ProtectTools Security Manager 管理者コンソール	• Security Manager セットアップ ウィザードは、セキュリティ レベルおよびセキュリティ ログイン方法をセットアップしたり設定したりするために管理者が使用します • 基本ユーザーからは非表示になっているオプションを設定します • Drive Encryption を有効にし、ユーザー アクセスを設定します • Device Access Manager の設定およびユーザー アクセスを設定します • 管理者ツールは、HP ProtectTools ユーザーの追加と削除、およびユーザーの状態の表示に使用します
HP ProtectTools Security Manager（一般ユーザー用）	• File Sanitizer のシュレッド、ブリーチ、および設定を構成および変更します • 暗号化の状態および Device Access Manager の設定を表示します • Privacy Manager を使用して、電子メールおよびドキュメントのセキュリティを向上させます • Computrace for HP ProtectTools を有効にします • [設定]オプションや[バックアップおよび復元]オプションを設定します
Credential Manager for HP ProtectTools（Security Manager の一部）	• ユーザー名およびパスワードを構成、設定、および変更します • Windows パスワードやスマート カードなどの、ユーザーの証明情報を設定および変更します • 個人用パスワードの保管場所として機能し、ユーザーの証明情報を自動的に記憶して適用する、シングルサインオン機能を使用してログオン プロセスを合理化します • シングルサインオンのユーザー名およびパスワードを作成および整理します
Drive Encryption for HP ProtectTools	• ボリューム全体にわたる完全なハードディスク ドライブの暗号化が可能です • ハードディスク ドライブ上のデータの暗号化解除やデータへのアクセスにブート前認証が使用されます • SED ドライブ（自己暗号化ドライブ）が搭載されている場合に、SED ドライブを有効にするオプションを提供します
Privacy Manager for HP ProtectTools	• Microsoft の電子メールおよび Microsoft Office ドキュメントを使用するときに、通信元、通信の整合性、および通信のセキュリティを確認するために、証明機関が発行する証明書を取得するために使用されます

モジュール	主な機能
File Sanitizer for HP ProtectTools	• コンピューター上のデジタル資産(アプリケーション ファイル、履歴や Web 関連情報、またはその他の機密データなど)を安全にシュレッドしたり、ハードディスク ドライブを定期的にブリーチ(以前に削除されたがハードディスク ドライブ上にはまだ存在するデータを上書きして、データの復元をさらに困難にすること)したりできます
Smart Card Security(Security Manager の一部)	• スマート カード用の管理ソフトウェア インターフェイスを提供します。HP ProtectTools Smart Card は、アクセスを許可するときにカードと PIN 番号の両方を要求して認証データを保護する個人用セキュリティ デバイスです。パスワード マネージャー、Drive Encryption、または任意の数の他社製アクセス ポイントにアクセスするときにスマート カードを使用することもできます • PIN 番号を変更します
Embedded Security for HP ProtectTools	• TPM(Trusted Platform Module)内蔵セキュリティ チップ(搭載されている場合)を使用して、コンピューター本体に保存されている機密のユーザー データまたは証明情報を不正なアクセスから保護するために役立ちます • ユーザーのファイルおよびフォルダー情報を保護するのに役立つ PSD(Personal Secure Drive)を作成できます • 保護されたデジタル証明情報を操作するための他社製のアプリケーション(Microsoft Outlook や Internet Explorer など)をサポートします
Device Access Manager for HP ProtectTools	• IT 管理者は、ユーザー プロファイルに基づいて、USB コネクタ、オプティカル ドライブ、個人用音楽プレーヤーなどのデバイスへのアクセスを制御できます • 不正なユーザーが外部のストレージ メディアを使用してデータを削除したり、外部のメディアからシステムにウィルスを侵入させたりできないようにします • 管理者は、特定の個人またはユーザーのグループに対して、書き込み可能なデバイスへのアクセスを無効にできます • ハードウェアへのアクセスを許可するスケジュールを管理者が設定できます
Computrace for HP ProtectTools	• 安全な資産情報管理を提供します • ユーザーの操作や、ハードウェアおよびソフトウェアの変更を監視できます • ハードディスク ドライブが再フォーマットまたは交換されてもアクティブな状態を維持します • 有効にするには、追跡およびトレース サブスクリプションを別途購入する必要があります

HP ProtectTools セキュリティ製品の説明と一般的な使用例

HP ProtectTools セキュリティ製品のほとんどは、パスワードを紛失したり、利用できなくなったり、忘れたりした場合、または企業のセキュリティ部門で必要となった場合にコンピューターにアクセスするためのユーザー認証機能（通常はパスワード）および管理バックアップ機能を搭載しています。

注記： 一部の HP ProtectTools セキュリティ製品は、データへのアクセスを制限するように設計されています。データの重要性が非常に高いためデータを紛失するより危険にさらすことの方が懸念される場合には、データを暗号化する必要があります。すべてのデータは安全な場所にバックアップしておくことをおすすめします。

Credential Manager（Password Manager）for HP ProtectTools

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）の一部である Credential Manager（証明書マネージャー）は、ユーザー名およびパスワードのリポジトリです。インターネット アクセスや Web メール用のログイン名およびパスワードを保存するために最もよく使用されます。Credential Manager を使用すると、ユーザーは Web サイトまたはメールに自動的にログインできます。

［**例 1**：］ある大規模メーカーの購買担当者は、その企業の取り引きのほとんどをインターネットで行っています。また、ログイン情報が必要となるいくつかの人気 Web サイトにもよくアクセスします。この購買担当者は、セキュリティに十分注意しているため、アカウントごとに異なるパスワードを使用しています。購買部では、Credential Manager を使用して、Web リンクごとに異なるユーザー名およびパスワードを設定することにしました。購買担当者が Web サイトのログイン画面にアクセスすると、Credential Manager によって資格情報が自動的に提供されます。ユーザー名およびパスワードが表示されるようにしたい場合は、Credential Manager で設定できます。

Credential Manager は、認証を管理および編集するためにも使用できます。このツールを使用すると、あらかじめ選択した Web 上またはネットワーク上の重要情報からどれかを選択し、そのリンクに直接アクセスできるようになります。また、必要に応じてユーザー名およびパスワードを表示することもできます。

［**例 2**：］ある多忙な公認会計士が、経理部全体を監督する立場に昇進しました。経理部では、多数のクライアントの Web アカウントに、それぞれ異なるログイン情報を使用してログインする必要があります。このログイン情報は複数の社員で共有する必要があるため、機密保持が問題となります。そこで、すべての Web リンク、企業ユーザー名、およびパスワードを Credential Manager for HP ProtectTools 内で整理することにしました。整理を完了させ、Credential Manager を社員に配布すれば、使用する資格情報を知らせないで社員に Web アカウントを利用させることができます。

Embedded Security for HP ProtectTools

Embedded Security for HP ProtectTools には、Personal Secure Drive を作成できる機能が搭載されています。この機能によって、ユーザーは、アクセスするまでは完全に非表示状態となる仮想ドライブ パーティションをコンピューター上に作成できます。Embedded Security（内蔵セキュリティ）は、他人に知られないように保護する必要があるデータと暗号化されていないデータが混在している場所で使用できます。

［**例 1**：］ある倉庫管理者はコンピューターを 1 台所有しており、複数の従業員が 1 日の間に何度かそのコンピューターにアクセスしています。管理者は、コンピューターに保存されている倉庫の機密データを暗号化し、表示されないようにしたいと考えています。また、たとえハードディスク ドライブを誰かに盗まれても、データは安全に保護され、そのデータを復号化されたり読み取られたりできないようにしたいと考えています。そこで、この倉庫管理者は、Embedded Security を有効にし、機密データを Personal Secure Drive に移動することにしました。この倉庫管理者はパスワードを入力すると、他のハードディスク ドライブとまったく同じように機密データにアクセスできます。管

理者がログオフするか Personal Secure Drive を再起動すると、正しいパスワードを入力しない限りデータを表示したり開いたりできなくなります。そのため、機密データが、コンピューターを使用する他の従業員の目に触れることはありません。

Embedded Security は、マザーボードに取り付けられているハードウェア TPM（Trusted Platform Module）内の暗号化キーを保護します。これは、復号化パスワードの推測によるパスワード攻撃に対抗できる最小要件を満たした唯一の暗号化ツールです。また、Embedded Security では、ドライブ全体および電子メールも暗号化できます。

［**例 2**：］ある証券ブローカーが、ポータブル ドライブを使用して、機密度の非常に高いデータを他のコンピューターに転送しようとしてます。たとえパスワードがわかったとしても、これら 2 台のコンピューター以外ではドライブを開けないようにしたいと考えています。そこで、この証券ブローカーは、Embedded Security TPM 移行機能を使用して、データを復号化するために必要な暗号化キーをもう 1 台のコンピューターに格納できるようにしました。これによって、パスワードがわかっている場合でも、データの移動処理中にデータを復号化できるのは、この 2 台の物理コンピューターのみとなります。

Drive Encryption for HP ProtectTools

Drive Encryption は、コンピューターのハードディスク ドライブ全体またはセカンダリ ハードディスク ドライブにあるデータへのアクセスを制限するためによく使用されます。Drive Encryption で SED ドライブ（自己暗号化ドライブ）を管理することもできます。

［**例 1**：］ある医師が、自分のコンピューターのハードディスク ドライブにあるどのデータにも自分しかアクセスできないようにしたいと考えています。そこで、この医師は Drive Encryption を有効にし、Windows のログイン前にブート前認証などの認証が求められるようにしました。セットアップを完了すれば、オペレーティング システムの起動前であっても、パスワードを入力しなければハードディスク ドライブを開くことはできなくなります。SED（自己暗号化ドライブ）オプションでデータを暗号化するように選択すれば、ドライブのセキュリティをさらに強化することもできます。

Embedded Security for HP ProtectTools および Drive Encryption for HP ProtectTools では、どちらも暗号化したデータをコンピューターのマザーボードに関連付けるため、たとえハードディスク ドライブを取り外してもそのデータにはアクセスできません。

［**例 2**：］ある病院の経営者は、医師および承認されている人だけが、個人パスワードを共有することなく、自分たちのコンピューター内のデータにアクセスできるようにしたいと考えています。そこで、病院の IT 部門は、その経営者、医師、および承認されたすべての人を Drive Encryption ユーザーとして追加することにしました。これで、承認された人だけが個人のユーザー名およびパスワードを使用してコンピューターまたはドメインにログオンできるようになります。

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools は、インターネット ブラウザーでの行動履歴、一時ファイル、以前に削除したデータ、および他のあらゆる情報が含まれたデータを完全に削除するために使用します。File Sanitizer は、手動で実行するか、またはユーザーが定義したスケジュールに従って自動実行するように設定できます。

［**例 1**：］ある弁護士は、クライアントの機密情報を頻繁に取り扱っており、削除したファイルのデータを復元できないようにしたいと考えています。そこで、この弁護士は削除済みファイルを File Sanitizer で「シュレッド」したため、データの復元はほぼ不可能になりました。

通常、Windows でデータを削除しても、データはハードディスク ドライブから完全に消去されるわけではありません。その代わりに、Windows はハードディスク ドライブのセクターに印を付け、将来そのセクターを使用できるようにします。そのため、データが上書きされるまでは、インターネッ

トで入手できる一般的なツールでそのデータを簡単に復元できます。File Sanitizer は、ランダムなデータをセクターに上書きするため（必要に応じて複数回実行します）、削除済みデータの読み取りや復元ができなくなります。

［**例 2**：］ある研究者は、削除済みデータ、一時ファイル、ブラウザーでの行動履歴などがログオフ時に自動でシュレッドされるようにしたいと考えています。そこで、File Sanitizer を使用して「シュレッド」のスケジュールを設定したため、一般的なファイルや独自のファイルを選択して自動的に完全消去できるようになりました。

Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools は、データのコピーが可能な USB フラッシュ ドライブへの不正なアクセスをブロックするために使用できます。また、CD/DVD ドライブへのアクセス、USB デバイスの制御、ネットワーク接続などを制限することもできます。管理者は、ドライブにアクセス可能な日時または期間をスケジュールすることもできます。例えば、外部の業者が社内のコンピューターにアクセスできるようにすると同時に、その業者がデータを USB ドライブにコピーできないようにする必要がある場合が考えられます。Device Access Manager for HP ProtectTools を使用すると、管理者はハードウェアへのアクセスを制限および管理できます。

［**例 1**：］医薬品会社のあるマネージャーは、個人の医療記録と会社のデータを仕事でよく使用しています。他の社員もこのデータにアクセスする必要がありますが、そのデータが USB デバイスや他の外部ストレージ メディアによってコンピューターからコピーされないようにすることが大変重要です。ネットワークは安全ですが、コンピューターに CD ライターや USB コネクタが搭載されているため、データがコピーされたり盗まれたりする可能性があります。そこで、このマネージャーは、Device Access Manager で CD ライターと USB コネクタを無効にし、使用できないようにしました。たとえ USB コネクタをブロックしても、マウスおよびキーボードは引き続き動作します。

［**例 2**：］ある保険会社では、社員が自宅にある個人のソフトウェアをインストールしたり、個人のデータを読み込んだりできないようにしたいと考えています。ただし、一部の社員は、すべてのコンピューターで USB コネクタにアクセスする必要があります。そこで、この会社の IT 管理者は、Device Access Manager を使用して、一部の社員に対してアクセスを許可すると同時に、その他の社員に対しては外部アクセスをブロックしました。

Privacy Manager for HP ProtectTools

Privacy Manager for HP ProtectTools は、インターネットでの電子メールのやり取りが安全に行われるようにするために使用します。ユーザーは、認証された相手しか開くことができない電子メールを作成および送信できます。Privacy Manager を使用すると、なりすましによって情報が危険にさらされたり、傍受されたりしないようにできます。

［**例 1**：］ある証券ブローカーは、自分の電子メールが特定のクライアントだけに送信され、他の何者かが電子メール アカウントを偽装してそのメールを傍受できないようにしたいと考えています。そこで、この証券ブローカーは、Privacy Manager を使用して自分と自分のクライアントの署名を登録しました。Privacy Manager は、各ユーザーの認証証明書を（CA）をユーザーに発行します。このツールを使用すると、証券ブローカーとクライアントは、電子メールをやり取りする前に認証する必要があります。

Privacy Manager for HP ProtectTools を使用すれば、確認および認証された相手と簡単に電子メールをやり取りできるようになります。また、メール サービスを暗号化することもできます。暗号化処理は、クレジット カードを使用した一般的なオンライン ショッピングと同じように行われます。

［**例 2**：］ある CEO は、自分が電子メールで送信した情報を取締役会のメンバーだけが閲覧できるようにしたいと考えています。そこで、この CEO は、取締役とやり取りする電子メールを暗号化する

ことにしました。Privacy Manager の認証証明書を使用すると、CEO と取締役は暗号化キーのコピーを取得し、機密性の高い電子メールを復号化できるようになります。

Computrace for HP ProtectTools（以前の LoJack Pro）

Computrace for HP ProtectTools は、盗難されたコンピューターがインターネットに接続されればいつでもその所在地を追跡できるサービスです。

[**例 1**：] ある学校の校長は、IT 部門に対し、学校にあるすべてのコンピューターを常時監視するように指示しました。そこで、学校の IT 管理者はコンピューターの保有状況を確認してから、すべてのコンピューターを Computrace に登録し、盗まれた場合に追跡できるようにしました。その後、この学校では、いくつかのコンピューターがなくなっていることに気づきました。そのため、IT 管理者は、警察に通報するとともに、Computrace の担当者に通知しました。これらのコンピューターは発見され、警察の手によって取り戻されて学校に返却されました。

Computrace for HP ProtectTools を使用すると、コンピューターをリモートで管理および特定したり、コンピューターの使用状況やアプリケーションを監視したりできます。

[**例 2**：] ある不動産会社では、世界中にあるコンピューターの管理および更新が必要になりました。そこで、Computrace を使用して、IT 担当者を実際に現地に派遣しなくてもコンピューターの監視および更新が実行できるようにしました。

HP ProtectTools セキュリティへのアクセス

Windows の[スタート]メニューから HP ProtectTools Security Manager にアクセスするには、以下の操作を行います。

▲ Windows で、[**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。

Windows の[スタート]メニューから HP ProtectTools Security Manager 管理者コンソールにアクセスするには、以下の操作を行います。

▲ Windows で、[**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。

注記： Password Manager モジュールを設定した後は、Windows のログオン画面から直接 Password Manager にログオンして HP ProtectTools を起動することもできます。

主なセキュリティの目的の実現

各 HP ProtectTools モジュールが連携して動作することによって、以下の主なセキュリティの目的を含む、さまざまなセキュリティの問題を解決できます。

- 盗難からの保護
- 機密データへのアクセス制限
- 内部または外部の場所からの不正なアクセスの防止
- 強力なパスワード ポリシーの作成
- セキュリティを義務付ける規制への対応

盗難からの保護

盗難の例として、コンピューターの盗難、またはコンピューターの機密データや顧客情報の盗難が挙げられます。こうした盗難は、職場や公共の場では容易に起こりうることです。コンピューターが盗まれた場合のデータの保護には、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスを防止することができます。以下の章を参照してください。
  - 28 ページの 「Password Manager for HP ProtectTools」
  - 58 ページの 「Embedded Security for HP ProtectTools」
  - 33 ページの 「Drive Encryption for HP ProtectTools」
- DriveLock は、ハード ディスク ドライブが取り外されてセキュリティ保護されていないシステムに取り付けられた場合でも、ドライブ上のデータにアクセスできないようにします。
- Embedded Security for HP ProtectTools モジュールによって提供される Personal Secure Drive 機能では、機密データを暗号化して、認証なしではアクセスできないようにします。以下の章を参照してください。
  - 58 ページの 「Embedded Security for HP ProtectTools」
- Computrace では、盗難の被害にあった後のコンピューターの場所を追跡できます。以下の章を参照してください。
  - 69 ページの 「Computrace for HP ProtectTools」

機密データへのアクセス制限

契約検査官がオンサイトで作業しており、機密の財務データの確認のためにコンピューターへのアクセスを許可されているとします。ただし、この検査官がこれらのファイルを印刷したり、CD などの書き込み可能なデバイスに保存できるようにはしたくありません。データへのアクセスを制限するには、以下の機能が役立ちます。

Device Access Manager for HP ProtectTools を使用すると、IT 管理者は書き込み可能なデバイスへのアクセスを制限して、機密の情報を印刷したり、ハードディスク ドライブからリムーバブル メディアにコピーしたりできないようにすることができます。65 ページの 「デバイス クラス構成（詳細設定）」を参照してください。

内部または外部の場所からの不正なアクセスの防止

セキュリティ保護されていないビジネス PC への不正なアクセスは、財務サービス、役員、または研究開発チームのデータなどの重要なデータや、カルテや個人の財務データなどの個人情報を非常に大きなリスクにさらすことになります。不正なアクセスを防止するには、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスを防止することができます。以下の章を参照してください。
  - 28 ページの 「Password Manager for HP ProtectTools」
  - 58 ページの 「Embedded Security for HP ProtectTools」
  - 33 ページの 「Drive Encryption for HP ProtectTools」
- Embedded Security for HP ProtectTools は、コンピューター本体に保存されている機密のユーザー データまたは証明情報の保護を強化できます。以下の章を参照してください。
  - 58 ページの 「Embedded Security for HP ProtectTools」
- Password Manager for HP ProtectTools は、不正なユーザーがパスワードを入手したり、パスワードで保護されたアプリケーションにアクセスしたりできないようにすることができます 。以下の章を参照してください。
  - 28 ページの 「Password Manager for HP ProtectTools」
- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は書き込み可能なデバイスへのアクセスを制限して、機密データをハードディスク ドライブからコピーできないようにすることができます。以下の章を参照してください。
  - 64 ページの 「Device Access Manager for HP ProtectTools」
- Personal Secure Drive 機能では、機密データを暗号化して、認証なしではアクセスできないようにします。以下の項目を参照してください。
  - 58 ページの 「Embedded Security for HP ProtectTools」
- File Sanitizer を使用すると、重要なファイルやフォルダーのシュレッドまたはハードディスク ドライブのブリーチ（以前に削除されたがハードディスク ドライブ上にはまだ存在するデータを上書きして、データの復元をさらに困難にすること）によって、データを安全に削除できます。以下の章を参照してください。
  - 50 ページの 「File Sanitizer for HP ProtectTools」
- Privacy Manager を使用すると、Microsoft メール、Microsoft Office ドキュメント、およびインスタント メッセンジャーを使用するときに証明機関が発行する証明書を取得して、重要な情報の送信と保存のプロセスを安全にすることができます。以下の章を参照してください。
  - 37 ページの 「Privacy Manager for HP ProtectTools」

強力なパスワード ポリシーの作成

いくつもの Web ベースのアプリケーションやデータベースに対して強力なパスワード ポリシーを使用する必要が生じた場合、Password Manager for HP ProtectTools は、パスワードやシングルサインオンのための保護されたリポジトリを提供します。以下の章を参照してください。

- 28 ページの 「Password Manager for HP ProtectTools」

その他のセキュリティ対策

セキュリティの役割の割り当て

コンピューターのセキュリティを管理する上では、責任および権限をさまざまな管理者やユーザーに割り当てることが、重要な作業の 1 つです。

注記： 小さな組織や個人で使用する場合は、1 人がすべての役割を持っていても構いません。

HP ProtectTools では、セキュリティの責任および権限を以下の役割に分割できます。

- セキュリティ統括責任者：企業またはネットワークのセキュリティ レベルを定義し、Drive Encryption や Embedded Security などの配備するセキュリティ機能を決定します。
- IT 管理者：セキュリティ統括責任者によって定義されたセキュリティ機能を適用し、管理します。また、一部の機能を有効または無効にできます。たとえば、セキュリティ統括責任者がスマート カードの配備を決定した場合、IT 管理者はパスワード モードおよびスマート カード モードの両方を有効にできます。
- ユーザー：セキュリティ機能を使用します。たとえば、セキュリティ統括責任者および IT 管理者がシステムでスマート カードを有効にしている場合、ユーザーはそのカードを認証に使用できます。

HP ProtectTools のパスワードの管理

HP ProtectTools Security Manager の機能のほとんどは、パスワードによってセキュリティ保護されています。以下の表に、よく使用されるパスワード、そのパスワードが設定されるソフトウェア モジュール、およびパスワード機能の一覧を示します。

この表には、IT 管理者だけが設定して使用するパスワードも示されています。その他のすべてのパスワードは、一般のユーザーまたは管理者が設定できます。

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
Password Manager のログオン パスワード	Password Manager	このパスワードには、以下の 2 つのオプションがあります • Windows にログオンした後、Password Manager にアクセスするための別のログオンで使用できます • Windows ログオン プロセスの代わりに使用し、Windows と Password Manager に同時にアクセスできます
基本ユーザー キーのパスワード **注記：** Embedded Security パスワードとも呼ばれます	Embedded Security	このパスワードを使用して、安全な電子メール、ファイル、フォルダーの暗号化などの Embedded Security 機能にアクセスします。電源投入時認証に使用すると、コンピューターの起動時や再起動時、またはハイバネーションからの復帰時にコンピューターのデータも保護されます
緊急リカバリ トークンのパスワード **注記：** 緊急リカバリ トークン キーとも呼ばれます	Embedded Security、IT 管理者が設定	内蔵セキュリティ チップ用のバックアップ ファイルである緊急リカバリ トークンへのアクセスを保護します

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
所有者のパスワード	Embedded Security、IT 管理者が設定	システムと TPM チップを、Embedded Security のすべての所有者機能への不正なアクセスから保護します
スマート カードの PIN	Smart Card Security	マルチファクター認証のオプションとして使用できます Windows 認証に使用できます スマート カード トークンが選択されている場合は、Drive Encryption のユーザーを認証します
コンピューター セットアップ(F10)ユーティリティのパスワード **注記：** BIOS の管理者パスワード、F10 セットアップ パスワード、またはセキュリティ セットアップ パスワードとも呼ばれます	BIOS、IT 管理者が設定	コンピューター セットアップ（F10）ユーティリティへのアクセスを保護します
電源投入時パスワード	BIOS	コンピューターの起動時や再起動時、またはハイバネーションからの復帰時にコンピューターのデータを保護します
Windows のログオン パスワード	Windows の[コントロール パネル]	手動ログオンに使用できます

安全なパスワードの作成

パスワードを作成する場合は、まず、プログラムで設定されている仕様に従う必要があります。ただし通常は、強力なパスワードを作成し、作成したパスワードが危険にさらされないようにするために、以下のガイドラインを参考にしてください。

- 文字数が 6 文字、できれば 8 文字を超えるパスワードを使用します。
- パスワード全体にわたって大文字と小文字を混在させます。
- 可能な場合は常に、半角英数字を混在させ、さらに特殊文字と句読点を含めます。
- パスワード中の文字の代わりに特殊文字または数字を使用します。たとえば、アルファベットの I または L の代わりに数字の 1 を使用します。
- 2 つ以上の言語から取った単語を組み合わせます。
- 単語またはフレーズを数字や特殊文字で分割します。たとえば、「Mary2-2Cat45」とします。
- 辞書に載っているような用語は使用しないでください。
- 名前やその他の個人情報（たとえば、誕生日、ペットの名前、母親の旧姓など）は、たとえ綴りを逆にしたとしても、パスワードには使用しないでください。
- パスワードは定期的に変更してください。いくつかの文字や数字を以下の値に変更するだけでも構いません。
- パスワードをメモした場合は、コンピューターのすぐ近くの、人目につきやすい場所に保管しないでください。
- パスワードを、電子メールなどのコンピューター上のファイルに保存しないでください。
- アカウントを共有したり、パスワードを誰かに教えたりしないでください。

証明情報および設定のバックアップ

以下の方法で証明情報をバックアップできます。

- Drive Encryption for HP ProtectTools を使用して、HP ProtectTools 証明情報の選択およびバック アップを行う

  オンラインの Drive Encryption キー復元サービスに登録して、暗号化キーのバックアップ コピーを保管することもできます。これによって、パスワードを忘れてしまい、ローカル バックアップにアクセスできない場合でも、コンピューターにアクセスできます。
- Embedded Security for HP ProtectTools を使用して、HP ProtectTools 証明情報をバックアップする
- HP ProtectTools Security Manager のバックアップと復元ツールを使用して、インストール済みの HP ProtectTools モジュールからセキュリティ証明情報のバックアップと復元をまとめて実行する

2　HP ProtectTools Security Manager 管理者コンソール

HP ProtectTools 管理者コンソールについて

HP ProtectTools Security Manager の管理は、管理者コンソールを通して提供されます。

このコンソールを使用すると、ローカル管理者は以下のことが可能になります。

- セキュリティ機能を有効または無効にする
- コンピューターのユーザーを管理する
- デバイス固有のパラメーターを調整する
- Security Manager アプリケーションを設定する
- Security Manager アプリケーションを追加する

管理者コンソールの使用

Security Manager 管理者コンソールは、HP ProtectTools Security Manager を管理するための中心となる場所です。

コンソールを開くには、以下の操作を行います。

- **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools 管理者コンソール]**の順に選択するか、または
- Security Manager コンソールの左下隅にある**[管理]**リンクをクリックします。

管理者コンソールは、左側のパネルおよび右側のパネルの 2 つのパネルで構成されています。左側のパネルには、管理ツールが含まれています。右側のパネルには、ツールを設定するための作業領域が含まれています。

管理者コンソールの左側のパネルは、以下の領域で構成されています。

- **[ホーム]**：セキュリティ機能の有効化、セキュリティ証明情報の指定、ユーザーの管理などの、よく使用されるタスクに容易にアクセスできるようにします。
- **[システム]**：システム全体のセキュリティ機能、ユーザー、およびスマート カード リーダーなどの認証デバイスの設定を管理します。
- **[アプリケーション]**：Security Manager およびそのアプリケーションの動作を設定するためのツールが含まれています。

- **[データ]**：ドライブの暗号化を管理したり、暗号化キーをバックアップおよび復元したりするためのツールを提供します。
- **[コンピューター]**：Device Access Manager が、PC のセキュリティを危険にさらす可能性のあるさまざまな種類のデバイスを個別に禁止したり、さまざまなユーザーおよびグループのアクセス権限を設定したりするための高度なセキュリティ オプションを提供します。
- **[通信]**：ユーザーが Privacy Manager を使用して電子メール認証用の第三者証明書を管理できます。また、Embedded Security を使用して、TPM で暗号化された電子メールをやり取りできます。
- **[管理ツール]**：初期設定のブラウザーで、Security Manager の機能を拡張するための追加の管理アプリケーションやツールを見つけることのできる Web ページを開きます。この Web ページでは、新しいアプリケーションやアップデートが使用可能になった場合は常に通知を受信するための方法もわかります。
- **[リンク]**：以下の機能を提供します。
  - **[セットアップ ウィザード]**：Security Manager の初期設定を実行できるセットアップ ウィザードを起動します。
  - **[ヘルプ]**：Security Manager およびそのアプリケーションに関する情報を提供するヘルプ ファイルを開きます。
  - **[バージョン情報]**：バージョン番号や著作権情報を含む、HP ProtectTools Security Manager に関する情報を表示します。

使用開始準備 - セットアップ ウィザード

HP ProtectTools Security Manager の管理には、管理者権限が必要です。

HP ProtectTools Security Manager セットアップ ウィザードを使用すると、HP ProtectTools のセキュリティ機能を設定できます。ただし、HP ProtectTools Security Manager コンソールを通して使用できる追加機能は豊富に存在します。このウィザードにあるのと同じ設定、および追加のセキュリティ機能は、Windows の[スタート]メニュー、または管理者コンソール内のリンクからアクセスするこのコンソールを通して設定できます。これらの設定は、コンピューターおよびそのコンピューターを共有するすべてのユーザーに適用されます。

初めて Windows にログオンすると、HP ProtectTools Security Manager を設定するよう求めるメッセージが表示されます。[**OK**]をクリックして、このプログラムを設定するための基本的な手順を実行できる Security Manager セットアップ ウィザードを起動します。

注記： 管理者コンソールの左側のパネルの一番下のセクションにある[**セキュリティ ウィザード**]をクリックすることによって、セキュリティ ウィザードを起動することもできます。

セットアップが完了するまで、セットアップ ウィザードの画面の説明に沿って操作します。

このウィザードを完了しない場合、[**今後、このウィザードを表示しない**]をクリックするまで、このウィザードが自動的に起動されます。

HP ProtectTools Security Manager アプリケーションを使用するには、[**スタート**]メニューから、またはタスクバー通知領域（システム トレイ）にある[**Security Manager**]アイコンを右クリックして HP ProtectTools Security Manager を起動します。Security Manager コンソールおよびそのアプリケーションは、このコンピューターを共有するすべてのユーザーが使用できます。

システムの設定

アプリケーションの[**システム**]グループは、管理者コンソールの左側にある[**ツール**]メニューからアクセスされます。

このグループに含まれているアプリケーションを使用すると、このコンピューター、そのユーザーおよびデバイスのポリシーや設定を設定したり管理したりすることができます。

[システム]グループには、以下のアプリケーションが含まれています。

- [**セキュリティ**]:セキュリティ機能、認証ポリシー、およびコンピューターまたはHP ProtectTools アプリケーションにログオンするときのユーザーの認証方法を管理するその他の設定を管理します。
- [**ユーザー**]:このコンピューターのユーザーを設定、管理、および登録します。
- [**デバイス**]:コンピューターに内蔵または接続されているセキュリティ デバイスの設定を管理します。

セキュリティ機能の有効化

ここで有効にしたセキュリティ機能は、このコンピューターのすべてのユーザーに適用されます。

1. 管理者コンソールの左側のパネルで、[**セキュリティ**]を展開し、[**機能**]をクリックします。
2. セキュリティ機能を有効にするには、[**Windows ログオンのセキュリティ**]か[**データの保護**](Drive Encryption を有効にします)、またはその両方の横にある対応するチェック ボックスにチェックを入れます。
   - [**Windows ログオンのセキュリティ**]:アクセスするために特定の証明情報の使用を要求することによって、Windows アカウントを保護します。
   - [**データの保護**]:Drive Encryption for HP ProtectTools を使用してハードディスク ドライブを暗号化し、適切な権限のないユーザーが情報を読み取れないようにすることによってデータを保護します。
3. [**次へ**]ボタンをクリックします。
4. [**完了**]ボタンをクリックします。

Security Manager 認証ポリシーの定義

このコンピューターの Security Manager 認証ポリシーは、ログオンおよびセッションの 2 つのタブで定義されます。これらのタブでは、ユーザー セッション中にコンピューターや HP ProtectTools アプリケーションにアクセスするときの各クラスのユーザーの認証に必要な証明情報を指定します。

[ログオン]タブ

コンピューターへのアクセス、ハードディスク ドライブの暗号化解除、および Windows へのログオンに必要な証明情報を指定するには、以下の操作を行います。

1. 管理者コンソールの左側のパネルで、[**セキュリティ**]を展開し、[**認証**]をクリックします。
2. [**ログオン**]タブで、ドロップダウン リストからユーザーのカテゴリを選択します。

3. [**ポリシー**]セクションで、一覧表示された証明情報の横にある、1 つ以上のチェック ボックスをクリックすることによって、選択したユーザーのカテゴリに必要な認証証明情報を指定します。少なくとも 1 つの証明情報を指定する必要があります。

4. [**ポリシー**]セクションのドロップダウン リストで、ユーザーを認証するために、指定した証明情報のどれか 1 つ（のみ）を要求するか、または指定した証明情報のすべてを要求するかを選択します。

5. [**適用**]ボタンをクリックします。

注記： ポリシーが[指定されたすべての証明情報が認証に必要]に設定され、パスワードとスマートカードの両方を使用するようにシステムが設定されているときに、スマート カードが破損しているか、または失われた場合は、すべての管理者が Windows からロックされ、アクセスを回復するには特殊なツールが必要になります。

[セッション]タブ

Windows セッション中に HP ProtectTools アプリケーションにログオンするときのユーザーの認証に必要な証明情報を管理するポリシーを定義するには、以下の操作を行います。

1. 管理者コンソールの左側のパネルで、[**セキュリティ**]を展開し、[**認証**]をクリックします。

2. [**セッション**]タブで、ユーザーのカテゴリを選択します。

3. [**ポリシー**]セクションで、一覧表示された証明情報の横にある、1 つ以上のチェック ボックスをクリックすることによって、選択したユーザーのカテゴリに必要な認証証明情報を指定します。少なくとも 1 つの証明情報を指定する必要があります。

4. [**ポリシー**]セクションのドロップダウン リストで、ユーザーを認証するために、指定した証明情報のどれか 1 つ（のみ）を要求するか、または指定した証明情報のすべてを要求するかを選択します。

5. [**適用**]ボタンをクリックします。

設定の定義

高度なセキュリティ設定のどれを許可するかを指定できます。設定を編集するには、以下の操作を行います。

1. 管理者コンソールの左側のパネルで、[**セキュリティ**]を展開し、[**設定**]をクリックします。

2. 特定の設定を有効または無効にするための適切なチェック ボックスにチェックを入れます。

3. [**適用**]をクリックして変更を保存します。

注記： [**ワン ステップ ログオンを許可する**]の設定を使用すると、BIOS または暗号化されたディスクのレベルで認証が実行された場合、このコンピューターのユーザーは Windows のログオンを省略できます。

ユーザーの管理

[ユーザー]アプリケーション内で、Windows 管理者はこのコンピューターのユーザー、およびそれらのユーザーに影響を与えるポリシーを管理できます。管理者コンソールで[ユーザー]アプリケーションにアクセスするには、**[ユーザー]**をクリックします。

HP ProtectTools ユーザーが一覧表示され、Security Manager で設定された認証ポリシー、およびこれらのポリシーを満たすために必要な証明情報に対して検証されます。

特定のユーザーに対して有効なポリシーを表示するには、一覧からユーザーを選択し、[**ポリシーの表示**]ボタンをクリックします。

証明情報を登録している間のユーザーを管理するには、一覧からユーザーを選択し、[**登録**]ボタンをクリックします。

ユーザーの追加

この処理によって、Drive Encryption のログオン リストにユーザーが追加されます。ユーザーを追加するには、そのユーザーがコンピューター上で Windows ユーザー アカウントをすでに与えられている必要があり、以下の手順の実行中にはそのアカウントが存在し、パスワードを入力できるようになっている必要があります。

ユーザーをユーザー リストに追加するには、以下の操作を行います。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 管理者コンソールの左側のパネルで、[**ユーザー**]を選択します。
3. [**追加**]ボタンをクリックします。[**ユーザーの選択**]ダイアログ ボックスが表示されます。
4. [**詳細**]→[**今すぐ検索**]ボタンの順にクリックして、追加するユーザーを検索します。
5. 一覧に追加するユーザーをクリックして[**OK**]をクリックします。
6. [**ユーザーの選択**]ダイアログ ボックスで[**OK**]をクリックします。
7. 選択したアカウントの Windows パスワードを入力して、[**完了**]をクリックします。

注記： Windows アカウントは既存のものを使用し、その名前を正しく入力する必要があります。このダイアログ ボックスで Windows ユーザー アカウントを変更または追加することはできません。

ユーザーの削除

注記： この手順を実行しても、Windows ユーザー アカウントは削除されません。Security Manager からアカウントが削除されるだけです。ユーザーを完全に削除するには、Security Manager と Windows の両方からユーザーを削除する必要があります。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 管理者コンソールの左側のパネルで、[**ユーザー**]を選択します。
3. 削除するアカウントのユーザー名をクリックし、[**削除**]をクリックします。
4. 確認用のダイアログ ボックスで[**はい**]をクリックします。

ユーザーの状態の確認

管理者コンソールの[ユーザー]セクションには、各ユーザーの現在の状態が表示されます。

- **[緑色のチェック マーク]**：必須のセキュリティ ログイン方法をそのユーザーが設定していることを示します。
- **[チルダ（~）]**：ユーザーが必須のセキュリティ ログイン方法を設定していないため、ログインしようとしてもコンピューターから拒否されることを示しています。このユーザーは、セットアップ ウィザードを実行して必須のログイン方法を設定する必要があります。
- **[表示なし]**：セキュリティ ログイン方法が必要ないことを示します。

デバイス設定の指定

[デバイス]アプリケーション内で、スマート カードが取り出されたら自動的にロックされるようにコンピューターを設定できます。ただし、コンピューターがロックされるのは、Windows へのログオン時にそのスマート カードが認証証明情報として使用された場合のみです。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 管理者コンソールの左側のパネルで、**[デバイス]**を展開し、**[スマート カード]**をクリックします。
3. スマート カードが取り出されたときのコンピューターのロックを有効または無効にするチェック ボックスにチェックを入れます。

アプリケーションの設定の構成

[設定]ウィンドウには、Security Manager およびそのアプリケーションの動作を設定するためのツールが含まれています。設定を変更するには、以下の操作を行います。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 管理者コンソールの左側のパネルで、**[設定]**を選択します。
3. **[全般]**タブで、HP ProtectTools Security Manager の全般的な設定を選択し、**[適用]**ボタンをクリックします。
4. **[アプリケーション]**タブで、有効または無効にするアプリケーションを選択し、**[適用]**ボタンをクリックします。

注記： アプリケーションを有効または無効にしても、コンピューターが再起動されるまで有効にならない場合があります。

ドライブの暗号化

Drive Encryption for HP ProtectTools を使用すると、コンピューターのハードディスク ドライブを暗号化することによって、そのハードディスク ドライブがコンピューターから取り外されたりデータ復旧サービスに送付されたりした場合でも、そのデータにアクセスしようとする不正なユーザーからの読み取りやアクセスを防ぐことができます。

Drive Encryption を有効または無効にするには、管理者コンソールで[セットアップ ウィザード]をクリックします。

Drive Encryption for HP ProtectTools の使用について詳しくは、33 ページの 「Drive Encryption for HP ProtectTools」を参照してください。

デバイス アクセスの管理

Device Access Manager for HP ProtectTools は、PC のセキュリティを危険にさらす可能性のあるさまざまな種類のデバイスを個別に禁止するための高度なセキュリティ オプションを提供します。Device Access Manager for HP ProtectTools の使用について詳しくは、64 ページの 「Device Access Manager for HP ProtectTools」を参照してください。

3 HP ProtectTools Security Manager

HP ProtectTools Security Manager を使用すると、コンピューターのセキュリティを大幅に向上させることができます。Security Manager アプリケーションを使用することで、以下のことが可能になります。

- ログオンおよびパスワードを管理する
- Windows パスワードを簡単に変更する
- 認証証明情報（スマート カードを含む）を設定する
- 電子メール、ドキュメント、およびインスタント メッセージングのプライバシやセキュリティを向上させる
- ハードディスク ドライブをシュレッドまたはブリーチする
- ドライブの暗号化の状態を表示する
- デバイス アクセスの設定を表示する
- 盗難からの回復ソフトウェアを有効にする
- Security Manager のデータをバックアップおよび復元する

Security Manager 設定後のログイン

ログインのシナリオは、Windows 管理者が設定時に選択したセキュリティ レベルとセキュリティ ログイン方法によって異なります。以下は、いくつかのシナリオ例です。

- すべてのセキュリティ レベルが設定され、**すべて**のセキュリティ ログイン方法が必須となっている場合、コンピューターの電源を最初に入れたときに、ユーザーは設定されているすべての方法でログインする必要があります。この操作を実行すると、ユーザーは Windows にログインされます。
- すべてのセキュリティ レベルが設定され、セキュリティ ログイン方法の**どれか 1 つ**だけで許可されるように設定されている場合、コンピューターの電源を最初に入れたときに、ユーザーは設定されているどれか 1 つのセキュリティ ログイン方法でログインできます。この操作を実行すると、ユーザーは Windows にログインされます。
- [HP Drive Encryption]レベルと[HP Password Manager]レベルのセキュリティが設定され、**すべて**のセキュリティ ログイン方法が必須となっている場合、[HP Drive Encryption]ログイン画面が表示されたときに、ユーザーは設定されているすべての方法でログインする必要があります。この操作を実行すると、ユーザーは Windows にログインされます。

- [HP Drive Encryption]レベルと[HP Password Manager]レベルのセキュリティが設定され、**どれか 1 つ**のセキュリティ ログイン方法だけで許可されるように設定されている場合、[HP Drive Encryption]ログイン画面が表示されたときに、ユーザーはどれか 1 つのセキュリティ ログイン方法でログインできます。この操作を実行すると、ユーザーは Windows にログインされます。
- [HP Password Manager]レベルのセキュリティが設定され、**すべて**のセキュリティ ログイン方法が必須となっている場合、[HP Password Manager]のログイン画面が表示されたときに、ユーザーは設定されているすべての方法でログインする必要があります。この操作を実行すると、ユーザーは Windows にログインされます。
- [HP Password Manager]レベルのセキュリティ オプションが設定され、設定されているセキュリティ ログイン方法の**どれか 1 つ**だけで許可されるように設定されている場合、[HP Password Manager]のログイン画面が表示されたときに、ユーザーはどれか 1 つのセキュリティ ログイン方法でログインできます。この操作を実行すると、ユーザーは Windows にログインされます。

注記： [HP Password Manager]レベルのセキュリティが設定されていない場合でも、他のセキュリティ レベルで求められるセキュリティ ログイン方法の種類に関わらず、ユーザーは Windows のログイン画面で Windows パスワードを入力する必要があります。

パスワードの管理

Password Manager for HP ProtectTools は、ログオンを作成および管理します。このログオンを使用すると、登録された証明情報で認証されることによって Web サイトを開いてログオンしたり、プログラムを起動してログオンしたりできます。

パスワードの管理について詳しくは、28 ページの 「Password Manager for HP ProtectTools」を参照してください。

証明情報の設定

Security Manager の証明情報は、ユーザーが実際に本人であることを確認するために使用します。このコンピューターのローカル管理者は、Windows アカウント、Web サイト、またはプログラムにログオンするときのユーザーの ID を証明するために使用できる証明情報を設定できます。

使用可能な証明情報は、コンピューターに内蔵または接続されているセキュリティ デバイスによって異なる場合があります。サポートされている証明情報は、それぞれ証明情報グループにエントリがあります。

Windows パスワードの変更

Security Manager での Windows パスワードの変更は、Windows の[コントロール パネル]を使用する場合よりも、簡単または迅速です。

Windows パスワードを変更するには、以下の操作を行います。

1. HP ProtectTools Security Manager の左側のパネルで、[**証明書**]をクリックします。
2. [**Windows パスワード**]をクリックします。
3. [**現在の Windows パスワード**]ボックスに現在のパスワードを入力します。

4. [**新しい Windows パスワード**]ボックスおよび[**新しいパスワードの確認**]ボックスに新しいパスワードを入力します。
5. [**変更**]をクリックします。

スマート カードの設定

スマート カードは Security Manager の一部です。スマート カードのセットアップおよび設定は、HP Smart Card キーボードから行います。スマート カードは、銀行の ATM でカードと暗証番号を併用するように、アクセスを許可するときにカードと PIN 番号の両方を要求して認証データを保護する個人用セキュリティ デバイスです。パスワード マネージャー、Drive Encryption PreBoot、または今後使用される他社製アクセス ポイントにアクセスするときにスマート カードを使用することもできます。スマート カードのオプションは、スマート カード リーダーが検出されるまで表示されません。

Smart Card Security を使用すると、以下のタスクを実行できます。

- スマート カードのセキュリティ機能にアクセスできます。
- Security Manager セットアップ ユーティリティと連携して、スマート カードの認証を有効にできます。
- Drive Encryption のブート前認証の方法としてスマート カードを使用できます。
- スマート カードを他の認証方法とともに使用できます。
- 管理者コンソールで PIN を初期化できます。

スマート カードの初期化

HP ProtectTools Security Manager では、多くの種類のスマート カードがサポートされています。PIN 番号として使用される文字の数および種類は、カードによって異なる場合があります。ProtectTools のセキュリティ アルゴリズムで使用されるセキュリティ証明書および管理用 PIN をインストールするためのツールは、スマート カードの製造元から提供されます。

注記： 多くの場合、製造元のスマート カード ソフトウェアによってロック解除キーが提供されています。ほとんどのスマート カードは、間違った PIN が 5 回入力されると自動的にロックされます。このキーはカードのロックを解除するために使用します。

1. 製造元のソフトウェアを使用してスマート カードをセットアップしたら、カードをリーダーに挿入します。
2. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
3. 管理者コンソールで、[**デバイス**]→[**スマート カードの使用の設定**]の順にクリックし、[**スマート カードのセットアップ**]タブをクリックします。
4. [**スマート カードの初期化**]が選択されていることを確認します。
5. **PIN** 番号を入力し、[**適用**]ボタンをクリックして、画面の説明に沿って操作します。
6. スマート カードが正常に初期化された後、スマート カードの登録に進みます。

スマート カードの登録

スマート カードを初期化した後、そのカードを管理者が管理者コンソールで認証方法として登録することも、ユーザーが Security Manager に登録することもできます。

管理者コンソールでスマート カードを登録するには、以下の操作を行います。

1. 管理者コンソールで、左下隅の[**セットアップ ウィザード**]をクリックします。
2. [**ようこそ**]画面で、[**次へ**]をクリックして Windows パスワードを入力します。
3. [**HP SpareKey**]ウィンドウで、[**[HP SpareKey]のセットアップのスキップ**]をクリックします（[HP SpareKey]の情報を更新しない場合）。
4. [**セキュリティ機能を有効にする**]ウィンドウで、[**次へ**]をクリックします。
5. [**資格情報の選択**]ウィンドウで、[**スマート カード**]が選択されていることを確認し、[**次へ**]をクリックします。
6. [**スマート カード**]ウィンドウで、**PIN** 番号を入力して[**次へ**]をクリックします。
7. [**完了**]をクリックします。

Security Manager でスマート カードを登録するには、以下の操作を行います。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。
2. Security Manager で、[**証明書**]を展開して、[**スマート カード**]をクリックします。
3. Windows パスワードと **PIN** 番号を入力し、[**保存**]をクリックします。

通信のプライバシの管理

Privacy Manager for HP ProtectTools によって、高度なセキュリティ ログイン（認証）方法を使用して、電子メール、Microsoft オフィス文書、またはインスタント メッセージング（IM）を使用するときの通信元、通信の整合性、および通信のセキュリティを確認できます。

Privacy Manager for HP ProtectTools について詳しくは、37 ページの 「Privacy Manager for HP ProtectTools」を参照してください。

ファイルのシュレッドまたはブリーチ

File Sanitizer for HP ProtectTools は、ファイルを意味のないデータで上書きすることによってファイルを削除します。「シュレッド」と呼ばれるこの処理によって、削除されたファイルの復元が非常に困難になるため、情報のセキュリティが大幅に向上します。File Sanitizer は、「ブリーチ」と呼ばれる処理を使用してハードディスク ドライブ上の以前に使用された領域を上書きすることによって、情報のセキュリティをさらに向上させます。File Sanitizer を使用して削除されたファイルを、オペレーティング システムやその他の一般に使用可能なファイル回復ソフトウェアで回復することはできません。

File Sanitizer for HP ProtectTools の使用について詳しくは、50 ページの 「File Sanitizer for HP ProtectTools」を参照してください。

ドライブの暗号化の状態の表示

ドライブの暗号化は、管理者コンソールで Windows 管理者によって設定されます。ユーザーは、Security Manager で自分の暗号化の状態を表示できます。

ドライブの暗号化の状態を表示するには、以下の操作を行います。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools Security Manager]**の順にクリックします。
2. Security Manager の左側のパネルで、**[Drive Encryption]**→**[暗号化の状態]**の順にクリックします。[暗号化の状態]ページには、ドライブの暗号化が有効になっているか無効になっているか、および各ドライブが暗号化されているかいないかが表示されます。

デバイス アクセスの表示

デバイス アクセスは、管理者コンソールで Windows 管理者によって設定されます。ユーザーは、Security Manager で自分のデバイス アクセスの設定を表示できます。

デバイス アクセスの設定を表示するには、以下の操作を行います。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools Security Manager]**の順にクリックします。
2. Security Manager の左側のパネルで、**[Device Access Manager]**を展開します。
3. アクセスを拒否されているデバイスを表示するには、**[簡易構成]**をクリックします。横にチェック マークが付いているデバイスは、アクセスを拒否されています。
4. アクセスを拒否されているユーザーまたはグループを表示するには、**[デバイス クラス構成]**をクリックします。
5. デバイスをクリックすると、そのデバイスへのアクセスを拒否または許可されているユーザーまたはグループが表示されます。

盗難からの回復の有効化

HP ProtectTools は、Absolute Software 社の Computrace を使用して、コンピューターをリモートから監視、管理、および追跡します。コンピューターの紛失または盗難が発生した場合は、Absolute 社の回復チームが回復に向けて当局と協力します。

Computrace の使用について詳しくは、69 ページの 「Computrace for HP ProtectTools」を参照してください。

アプリケーションの追加

追加のアプリケーションを使用して、このプログラムに新機能を追加できます。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools Security Manager]**の順にクリックします。
2. Security Manager の左側のパネルで、**[管理]**ドロップダウン メニューを選択して、**[他を検出]**をクリックします。

注記： **[他を検出]**リンクがない場合は、コンピューターの管理者によってこのリンクが無効にされています。

3. **[アプリケーションの追加]**タブで、追加のアプリケーションを参照します。
4. **[更新およびメッセージ]**タブで、**[新しいアプリケーションおよび更新に関する通知を受け取る]**チェック ボックスにチェックを入れてアップデートを確認する日数を設定することによって、新しいアプリケーションやアップデートに関する通知を常に受信することができます。または、**[今すぐチェック]**ボタンをクリックして、アップデートをすぐに確認することもできます。

設定のオプション

[設定]ページでは、**[アイコンをタスクバーに表示]**チェック ボックスにチェックを入れて、タスクバー通知領域（システム トレイ）に[Security Manager]アイコンを表示できます。

[設定]ページにアクセスするには、以下の操作を行います。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools Security Manager]**の順にクリックします。
2. Security Manager の左側のパネルで、**[詳細]**→**[設定]**の順にクリックします。
3. **[アイコンをタスクバーに表示]**チェック ボックスのチェックを入れるか、チェックを外して**[適用]**をクリックします。

バックアップおよび復元

Security Manager のデータは定期的にバックアップすることをおすすめします。バックアップの頻度は、データが変更される頻度によって異なります。たとえば、新しいログオンを毎日のように定期的に追加している場合は、おそらく毎日データをバックアップする必要があります。

バックアップは、あるコンピューターから別のコンピューターへ移行するためにも使用できます（インポートおよびエクスポートとも呼ばれます）。ただし、この機能では、データのみがバックアップされることに注意してください。

バックアップ ファイルを別のコンピューターに復元する場合や、オペレーティング システムの再インストール後に同じコンピューターに復元する場合は、バックアップ ファイルからデータを復元する前に、HP ProtectTools Security Manager がすでにそのシステムにインストールされている必要があります。

データのバックアップ

データをバックアップする場合は、ログオンおよび証明情報を、入力したパスワードで保護された暗号化ファイルに保存します。

データをバックアップするには、以下の操作を行います。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。
2. Security Manager の左側のパネルで、[**詳細**]→[**バックアップおよび復元**]の順にクリックします。
3. [**データのバックアップ**]をクリックします。
4. バックアップに含めるモジュールを選択します。多くの場合、すべてのモジュールの選択が必要になります。[**次へ**]をクリックします。
5. ID を確認するためのパスワードを入力し、矢印ボタンをクリックします。
6. ストレージ ファイルのパスおよび名前を入力します。初期設定では、ファイルはドキュメントフォルダーに保存されます。別の場所を指定するには、[**参照**]をクリックします。[**次へ**]をクリックします。
7. ファイルを保護するには、パスワードの入力と確認を行います。
8. [**完了**]をクリックします。

データの復元

Security Manager のバックアップおよび復元機能を使用して以前に作成された、パスワードで保護された暗号化ファイルからデータを復元します。

データを復元するには、以下の操作を行います。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。
2. Security Manager の左側のパネルで、[**詳細**]→[**バックアップおよび復元**]の順にクリックします。
3. [**データの復元**]をクリックします。
4. ストレージ ファイルのパスおよび名前を入力するか、または[**参照**]をクリックしてファイルを選択します。
5. ファイルを保護するために使用されたパスワードを入力し、[**次へ**]をクリックします。
6. データを復元するモジュールを選択します。多くの場合、一覧表示されているすべてのモジュールを選択することになります。[**次へ**]をクリックします。
7. [**完了**]をクリックします。

Windows のユーザー名および画像の変更

Security Manager の左上隅には、Windows のユーザー名と画像が表示されます。

ユーザー名や画像を変更するには、以下の操作を行います。

1. ユーザー名および画像がある Security Manager の左上のセクションをクリックします。
2. ユーザー名を変更するには、［**Windows ユーザー名**］ボックスに名前を入力します。
3. 画像を変更するには、［**画像の選択**］ボタンをクリックし、画像を参照して選択します。
4. ［**保存**］ボタンをクリックして変更内容を保存します。

4 Password Manager for HP ProtectTools

Password Manager を使用すると、Windows、Web サイト、およびプログラムへのログオンがより簡単かつ安全になります。

Password Manager では、Web サイトおよびプログラムにすばやく安全にアクセスできるようにするため、Web サイトおよびプログラムのログオン画面を設定できます。Password Manager は、まずログオンを認識し、各ログオン画面の入力ボックスに入力された個々のデータを記憶します。その後、ログオン画面が表示されると、Password Manager はユーザーの ID を確認し、そのデータを自動的に入力および送信します。

ホットキーの組み合わせを設定（初期設定は Ctrl ＋ Alt ＋ H）して使用すると、すぐにログオン メニューが表示されるため、さらにすばやいアクセスが可能になります。メニューでは、ログオンを選択するだけで Password Manager が Web サイトまたはプログラムを起動し、ログオン画面に移動して自動的にログインを実行します。

ID を確認するには、Windows パスワードやスマートカードなど、お使いのコンピューターの構成に適した HP ProtectTools 証明情報を使用します。つまり、設定したどのログオン画面でも、同じ証明情報を使用してログオンすることになります。したがって、書き留めておいたり覚えておいたりする必要がない強固なパスワードを作成して、アカウントをより安全にすることができます。

Password Manager では、お使いのパスワードにセキュリティ上のリスクがあるかどうかを一目でわかる形で表示し、新しいサイト用に複雑で強力なパスワードを自動作成できます。

また、Password Manager では、パスワードなどのログオン情報を表示して、いつでも編集することができます。あらかじめ設定したプログラムまたは任意の Web サイトのログオン画面がフォーカスされているときに必ず表示される[パスワード マネージャー]アイコンからも、Password Manager の多くの機能を利用できます。アイコンをクリックするとコンテキスト メニューが表示され、このメニューから以下のオプションを選択できます。

ログオンが作成されていない Web ページまたはプログラムの場合：

以下のオプションがコンテキスト メニューに表示されます。

- [[任意のドメイン]をパスワード マネージャーに追加]：表示中のログオン画面用にログオンを追加するために使用します。
- [[パスワード マネージャー]を開く]：[パスワード マネージャー]ページで Security Manager を起動します。

- [[パスワード マネージャー]アイコンの設定]：[パスワード マネージャー]アイコンを表示する条件を指定できます。
- [ヘルプ]：Password Manager アプリケーションのオンライン ヘルプを表示します。

ログオンが作成されている Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。

- [ログオン データの入力]：ログオン データをログオン用フィールドに入力してページを送信します（ログオンを作成または最後に編集したときに送信を指定していた場合）。
- [ログオンの編集]：表示中の Web サイト用のログオン データを編集できます。
- [ログオンの追加]：同じ Web サイトまたはプログラムに別のログオンを追加するために使用します。
- [パスワード マネージャーを起動]：[パスワード マネージャー]ページで Security Manager ダッシュボードを起動します。
- [ヘルプ]：Password Manager アプリケーションのオンライン ヘルプを表示します。

注記： Security Manager は、証明情報を確認するときに、複数の証明情報を要求するようにコンピューターの管理者によってセットアップされていることがあります。

ログオンの追加

Web サイトまたはプログラム用のログオンは、すばやく簡単に追加できます。サイトまたはプログラムのログオン情報を 1 回入力すれば、以降は Password Manager によって情報が自動的に入力されるようになります。これらのログオンは、その Web サイトまたはプログラムを表示すると使用できるようになります。また、[ログオン]メニューからログオンを選択し、Password Manager によってその Web サイトまたはプログラムを表示してログオンすることもできます。

ログオンを追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. [パスワード マネージャー]アイコンの矢印をクリックし、ログオン画面の種類（Web サイト用またはプログラム用）に応じて以下のどちらかを選択します。
   - Web サイトの場合：**[[任意のドメイン]をパスワード マネージャーに追加]**を選択します。
   - プログラムの場合：**[このログオン画面をパスワード マネージャーに追加]**を選択します。
3. ログオン データを入力します。画面のログオン用フィールドおよびダイアログの対応するフィールドが、オレンジ色の太い枠線で識別されます。Password Manager の**[管理]**タブから[ログオンの追加]を選択するなどして、このダイアログを表示するための、他のオプションを利用することもできます。Ctrl ＋ H ホットキーを使用したりスマート カードを挿入したりするなど、コンピューターに接続されているセキュリティ デバイスに依存するオプションもあります。
   - あらかじめフォーマットが用意された選択肢の 1 つを使用してログオン用フィールドに入力するには、フィールドの右側にある矢印をクリックします。
   - 必要に応じて画面上の他のフィールドをログオンに追加するには、**[他のフィールドの選択]**をクリックします。

- ログオン用フィールドの入力後に送信を実行しない場合は、[**ログオン データの送信**]の選択を解除します。
- このログオン用のパスワードを表示するには、[**パスワードの表示**]をクリックします。

4. [**OK**]をクリックします。[パスワード マネージャー]アイコンのプラス記号（＋）が消え、ログオン情報が作成されたことが示されます。
5. Windows パスワードを入力して緑の矢印をクリックします。

これで、その Web サイトにアクセスするかそのプログラムを起動すると、その度に[パスワード マネージャー]アイコンが表示され、登録済みの証明情報を使用してログオンできることが示されるようになります。

ログオンの編集

ログオンを編集するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. [パスワード マネージャー]アイコンの矢印をクリックし、[**ログオンの編集**]を選択して、ログオン情報を編集できるダイアログを表示します。画面のログオン用フィールドおよびダイアログの対応するフィールドが、オレンジ色の太い枠線で識別されます。
3. Windows パスワードを入力して緑の矢印をクリックします。
4. ログオン情報を編集します。
   - あらかじめフォーマットが用意された選択肢の 1 つを使用してログオン用フィールドに入力するには、フィールドの右側にある矢印をクリックします。
   - 必要に応じて画面上の他のフィールドをログオンに追加するには、[**他のフィールドの選択**]をクリックします。
   - ログオン用フィールドの入力後に送信を実行しない場合は、[**アカウント データの送信**]の選択を解除します。
   - このログオン用のパスワードを表示するには、[パスワードを表示する]をクリックします。このパスワードを表示するには、Windows パスワードが必要です。
5. [**OK**]をクリックします。

ログオン メニューの使用

パスワード ネージャでは、ログオンを作成した Web サイトおよびプログラムをすばやく簡単に起動できます。[ログオン]メニューまたは[パスワード マネージャー]の[**管理**]タブからプログラムまたは Web サイトをダブルクリックし、ログオン画面を表示して、ログオン データを入力します。初期設定では、ログオン情報もすぐに Web サイトに送信されます。ただし、最初の設定時またはログオンの編集時に[**アカウント データの送信**]の選択を解除して、送信されないようにすることができます。

作成したログオンは、Password Manager の[ログオン]メニューに自動的に追加されます。

[ログオン]メニューを表示するには、パスワード マネージャーのホットキーを押します。初期設定では Ctrl ＋ Windows キー＋ H ですが、[**パスワード マネージャー**]→[Windows パスワード]→緑の矢印→[**設定**]の順にクリックしてホットキーの組み合わせを変更できます。

ログオンをカテゴリ別に整理

ログオンを整理するには、カテゴリを使用します。1 つ以上のカテゴリを作成し、ログオンを目的のカテゴリにドラッグ アンド ドロップするのみで簡単に整理できます。

カテゴリを追加するには、以下の操作を行います。

1. Security Manager の左側のパネルで、[**パスワード マネージャー**]を選択します。
2. [**管理**]タブを選択し、[**カテゴリの追加**]をクリックします。
3. カテゴリの名前を入力します。
4. [**OK**]をクリックします。

ログオンをカテゴリに追加するには、以下の操作を行います。

1. マウス ポインターを目的のログオンの上に置きます。
2. マウスの左ボタンを押したままにします。
3. ログオンをカテゴリの一覧にドラッグします。マウス ポインターをカテゴリの上に置くと、そのカテゴリが強調表示されます。
4. 目的のカテゴリが強調表示されたら、マウス ボタンを放します。

ログオンは、選択したカテゴリに移動されるのではなく、コピーされるのみです。そのため、同じログオンを複数のカテゴリに追加できます。[**すべて**]をクリックすると、常にすべてのログオンを表示できます。

ログオンの管理

Password Manager を使用すると、ユーザー名、パスワード、および複数のログオン アカウントのログオン情報を、中心となる 1 つの場所から簡単かつ直感的に管理できます。

ログオンは[**管理**]タブに一覧表示されます。同じ Web サイトに対して複数のログオンが作成されている場合、各ログオンは常にその Web サイト名の下に一覧表示され、ログオン一覧の中でインデント表示されます。

ログオンを管理するには、以下の操作を行います。

Security Manager の左側のパネルで、[**パスワード マネージャー**]を選択して、[**管理**]タブをクリックします。編集する Web サイトを開きます。

- ログオンの追加：[**ログオンの追加**]をクリックし、画面の説明に沿って操作します。
- ログオンの編集：ログオンを選択して[**編集**]をクリックします。ログオン データを目的に合うように変更します。
- ログオンの削除：ログオンを選択して[**削除**]をクリックします。

Web サイトまたはプログラムに他のログオンを追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. [パスワード マネージャー]アイコンをクリックして、ショートカット メニューを表示します。
3. [**他のログオンの追加**]を選択し、画面の説明に沿って操作します。

パスワード強度の評価

証明情報を保護するには、Web サイトおよびプログラムに強固なパスワードを使用することが重要です。

Password Manager では、Web サイトおよびプログラムへのログオンに使用されている各パスワードの強度を自動的にすばやく分析することで、セキュリティを簡単に監視および強化できます。ログオンに使用するパスワードの強度は、Password Manager の[**パスワード強度**]タブで確認できます。

[パスワード マネージャー]アイコンの設定

Password Manager では、Web サイトおよびプログラムのログオン画面の識別が試行されます。ログオンが作成されていないログオン画面が検出されると、Password Manager によってプラス記号（+）の付いた[パスワード マネージャー]アイコンが表示され、その画面用のログオンを追加するよう求められます。

以下の設定を実行できます。

- [常に要求する]：ログオンがまだ設定されていないログオン画面が表示されたときに、Password Manager によってログオンの追加を必ず求められるようにするには、このオプションを選択します。
- [この画面では要求しない]：Password Manager によってこの特定のログオン画面へのログオンの追加を今後求められないようにするには、このオプションを選択します。
- [常に要求しない]：セットアップされていないログオン画面に対して、Password Manager によって何も求められないようにするには、このオプションを選択します。

Security Manager で、[**パスワード マネージャー**]→[Windows パスワード]→緑の矢印→[**設定**]の順に選択すると、Privacy Manager の詳細設定を利用できます。

5 Drive Encryption for HP ProtectTools

注記： Drive Encryption for HP ProtectTools は、一部のモデルでのみ利用できます。

今日では、会社にある自分のコンピューターや他の社員のコンピューターが盗まれて、企業の重要な情報が大きな危険にさらされる可能性があります。コンピューターのハードディスク ドライブ上のデータをすべて暗号化すれば、不正なユーザーがそのデータにアクセスしようとして、ドライブをコンピューターから取り外したりデータ復旧サービスに送ったりしても、読み取ったりアクセスしたりできないようになります。

Drive Encryption for HP ProtectTools ソフトウェアは、ボリューム全体をすぐに暗号化できる機能を業界で初めて搭載しています。ハードディスク ドライブを暗号化することによって完全なデータ保護を可能にします。Drive Encryption を有効にしている場合は、Windows が起動する前に表示される Drive Encryption のログイン画面からログインする必要があります。

注記： Drive Encryption for HP ProtectTools の有効化は、HP ProtectTools 管理者コンソールのセットアップ ウィザードからのみ実行できます。

注記： Drive Encryption は、AMD 製プロセッサを使用するシステムで、RAID 構成されている 64 ビット オペレーティング システムではサポートされていません。

Drive Encryption では、以下の作業を実行できます。

- 内蔵ハードディスク ドライブのすべてのデータを暗号化
- パスワードによる簡単なアクセスおよびブート前認証
- Microsoft Windows XP、Windows Vista®、および Windows 7 をサポート
- TPM（Trusted Platform Module）内蔵セキュリティ チップの使用（セキュリティ チップがコンピューターに搭載されていて、TPM での設定が行われている場合）

Drive Encryption for HP ProtectTools では、以下のような、さまざまなタスクを実行できます。

- Drive Encryption の管理
    - TPM で保護されたパスワードの有効化
    - 個々のドライブの暗号化または暗号化の解除
    - 自己暗号化ドライブ（SED）の有効化
- バックアップおよび復元
    - バックアップ キーの作成
    - オンライン復元の登録
    - 既存のオンライン復元アカウントの管理
    - 復元の実行

△ **注意：** Drive Encryption モジュールをアンインストールする場合、またはバックアップと復元用のソリューションを使用している場合は、まず暗号化されたすべてのドライブの暗号化を解除する必要があります。そうしないと、Drive Encryption 復元サービスに登録していない限り、暗号化されたドライブ上のデータにアクセスできなくなります。Drive Encryption モジュールを再インストールしても、暗号化されたドライブにはアクセスできません。

セットアップ手順

Drive Encryption を開く

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. **[ドライブの暗号化]**をクリックします。

一般的なタスク

Drive Encryption の有効化

Drive Encryption を有効にするには、HP ProtectTools 管理者コンソール セットアップ ウィザードを使用します。

Drive Encryption の無効化

Drive Encryption を無効にするには、HP ProtectTools 管理者コンソール セットアップ ウィザードを使用します。

Drive Encryption の有効化後のログイン

Drive Encryption を有効にし、ユーザー アカウントを登録した後でコンピューターを起動した場合は、Drive Encryption のログオン画面からログインする必要があります。

注記： Windows 管理者が HP ProtectTools 管理者コンソールでブート前セキュリティを有効にしている場合は、Drive Encryption のログオン画面が表示されたときではなく、コンピューターの電源を入れた直後コンピューターにログインされます。

1. ユーザー名を選択し、Windows パスワードまたはスマート カードの PIN を入力します。
2. [**OK**]をクリックします。

注記： Drive Encryption のログオン画面で復元キーを使用してログオンする場合は、Windows のログオン画面で Windows のユーザー名を選択し、パスワードを入力することも要求されます。

高度なタスク

Drive Encryption の管理（管理者のタスク）

[Drive Encryption]ウィンドウでは、Windows 管理者は Drive Encryption の状態（有効または無効）を表示および変更し、コンピューター上のすべてのハードディスク ドライブの暗号化の状態を表示できます。

TPM で保護されたパスワードの有効化

TPM を有効にするには、Embedded Security for HP ProtectTools を使用します。有効にした後、Drive Encryption のログオン画面でログインするには、Windows のユーザー名をパスワードが必要になります。

注記： パスワードは TPM セキュリティ チップで保護されているため、ハードディスク ドライブを別のコンピューターに移動すると、TPM 設定をそのコンピューターに移行しない限り、データにアクセスできなくなります。

1. TPM を有効にするには、Embedded Security for HP ProtectTools を使用します。
2. 管理者コンソールの左側のパネルで、[**Drive Encryption**]を展開して、[**暗号化の管理**]をクリックします。
3. [**TPM でセキュリティを強化**]チェック ボックスにチェックを入れます。

個々のドライブの暗号化または暗号化の解除

1. 管理者コンソールの左側のパネルで、[**Drive Encryption**]を展開して、[**暗号化の管理**]をクリックします。
2. [**暗号化の変更**]ボタンをクリックします。
3. [暗号化の変更]ダイアログ ボックスで、暗号化するか、暗号化を解除する各ハードディスク ドライブの横にあるチェック ボックスにチェックを入れるか、またはチェックを外して、[**OK**]をクリックします。

注記： ドライブの暗号化または暗号化解除が行われている間、現在のセッションで処理が完了するまでの残り時間が進行状況バーに表示されます。暗号化中にコンピューターをシャットダウンするか、スリープまたはハイバネーションを開始してから起動しなおした場合、残り時間の表示はリセットされますが、実際の暗号化は直前に停止した場所から再開されます。残り時間と進行状況の表示がすばやく進み、現在の進行状況が反映されます。

バックアップおよび復元（管理者のタスク）

Drive Encryption の[バックアップおよび復元]ウィンドウでは、Windows 管理者が暗号化キーをバックアップし、復元することができます。

バックアップ キーの作成

△ **注意：** バックアップ キーを含むストレージ デバイスは必ず安全な場所に保管してください。パスワードを忘れたり、スマート カードを紛失したりした場合は、このデバイスがハードディスク ドライブにアクセスする唯一の方法となります。

1. 管理者コンソールの左側のパネルで、[**Drive Encryption**]を展開して、[**バックアップおよび復元**]をクリックします。
2. [**キーをバックアップする**]ボタンをクリックします。
3. [バックアップ ディスクの選択]ページで、暗号化キーをバックアップするデバイスの名前をクリックし、[**次へ**]をクリックします。
4. 次に表示されるページの情報を確認してから、[**次へ**]をクリックします。

   選択したストレージ デバイスに暗号化キーが保存されます。
5. 確認ダイアログ ボックスが表示されたら、[**OK**]をクリックします。

注記： 復元の管理および実行について詳しくは、Drive Encryption for HP ProtectTools のヘルプ ファイルを参照してください。

6　Privacy Manager for HP ProtectTools

Privacy Manager は証明機関が発行する証明書の取得に使用するツールで、Microsoft メール、Microsoft Office ドキュメント、およびインスタント メッセンジャーを使用するときに、通信元、通信の整合性、および通信のセキュリティを確認します。

Privacy Manager は、HP ProtectTools Security Manager が提供するセキュリティ インフラストラクチャを利用します。このインフラストラクチャには以下のセキュリティ ログイン方法が含まれています。

- Windows のパスワード
- スマート カード

Privacy Manager では、上記のセキュリティ ログイン方法を使用できます。

Privacy Manager の起動

Privacy Manager を起動するには、以下の操作を行います。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。
2. Security Manager の左側のパネルで、[**Privacy Manager**]をクリックします。

または

タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを右クリックしてから、[**Privacy Manager for HP ProtectTools**]を強調表示して、[**構成**]をクリックします。

または

Microsoft Outlook の電子メール メッセージのツールバーで[**安全に送信**]の横にある下向きの矢印をクリックしてから、[**証明書マネージャー**]または[**信頼済み連絡先マネージャー**]をクリックします。

または

Microsoft Office ドキュメントのツールバーで[**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**証明書マネージャー**]または[**信頼済み連絡先マネージャー**]をクリックします。

セットアップ手順

Privacy Manager の証明書の管理

Privacy Manager の証明書は、公開キー基盤（PKI）と呼ばれる暗号化技術を使用して、データとメッセージを保護します。PKI の利用にあたり、ユーザーは暗号キーと、証明機関（CA）が発行する Privacy Manager の証明書を取得する必要があります。認証を定期的に要求するだけのほとんどのデータ暗号化ソフトウェアや認証ソフトウェアとは異なり、Privacy Manager は、暗号キーを使用して電子メール メッセージや Microsoft Office ドキュメントに署名するたびに認証を要求します。Privacy Manager によって、重要な情報の保存と送信の処理が安全で確実なものとなります。

Privacy Manager の証明書の要求とインストール

Privacy Manager の機能を使用するには、有効な電子メール アドレスを使用して Privacy Manager から Privacy Manager の証明書を要求し、インストールしておく必要があります。この電子メール アドレスは、Privacy Manager の証明書を要求するコンピューターの Microsoft Outlook のアカウントとして設定する必要があります。

Privacy Manager の証明書の要求

1. Security Manager の左側のパネルで、［**Privacy Manager**］を展開して、［**証明書**］をクリックします。
2. ［**Privacy Manager の証明書の要求**］ボタンをクリックします。
3. [ようこそ]ページで、画面に表示される内容を確認してから[**次へ**]をクリックします。
4. [使用許諾契約]ページで、使用許諾契約の内容を確認します。
5. ［**使用許諾契約の条件に同意する場合はチェック**］の隣のチェック ボックスにチェックが入っていることを確認してから、［**次へ**］をクリックします。
6. [証明書の詳細]ページで、求められた情報を入力してから[**次へ**]をクリックします。
7. [証明書の要求が承認されました]ページで、［**完了**］をクリックします。

   Microsoft Outlook に、Privacy Manager の証明書が添付された電子メールが届きます。

Privacy Manager の証明書のインストール

1. Privacy Manager の証明書の添付された電子メールを受信したら、メールを開き、メッセージの右下隅にある［**設定**］ボタンをクリックします。
2. 選択したセキュリティ ログイン方法で認証します。
3. [証明書がインストールされました]ページで、［**次へ**］をクリックします。
4. [証明書のバックアップ]ページで、バックアップ ファイルの保存先と名前を入力するか、または［**参照**］をクリックして保存先を探します。

   △ **注意：** ファイルはハードディスク ドライブ以外の場所に保存し、安全な場所に保管してください。本人以外はこのファイルを使用できません。また、Privacy Manager の証明書と、関連するキーを復元しなければならない場合には、このファイルが必要です。

5. パスワードの入力と確認を行い、［**次へ**］をクリックします。

6. 選択したセキュリティ ログイン方法で認証します。

7. 信頼済み連絡先の招待の処理を始める場合は、画面の説明に沿って操作します。

   または

   [キャンセル]をクリックすると、後で信頼済み連絡先を追加できます。詳しくは、「信頼済み連絡先の管理」を参照してください。

Privacy Manager の証明書の詳細の表示

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**証明書マネージャー**]をクリックします。

2. [**Privacy Manager の証明書**]をクリックします。

3. [**証明書の詳細**]をクリックします。

4. 詳細の確認を終えたら、[**OK**]をクリックします。

Privacy Manager の証明書の更新

Privacy Manager の証明書が有効期限に近づくと、更新が必要であることが通知されます。

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**証明書マネージャー**]をクリックします。

2. [**Privacy Manager の証明書**]をクリックします。

3. [**証明書の更新**]をクリックします。

4. 画面の説明に沿って操作し、新しい Privacy Manager の証明書を購入します。

   注記： Privacy Manager の証明書の更新処理を行っても、古い Privacy Manager の証明書は置き換えられません。新しい Privacy Manager の証明書を購入したら、「Privacy Manager の証明書の要求とインストール」に記載されている手順でインストールする必要があります。

Privacy Manager の証明書の初期設定の指定

お使いのコンピューターに別の証明機関からの証明書がインストールされている場合でも、Privacy Manager には Privacy Manager の証明書のみが表示されます。

コンピューターに Privacy Manager からインストールした Privacy Manager の証明書が複数ある場合は、どれか 1 つを初期設定の証明書として指定できます。

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**証明書マネージャー**]をクリックします。

2. 初期設定として使用する Privacy Manager の証明書をクリックしてから、[**初期値の指定**]をクリックします。

3. [**OK**]をクリックします。

注記： 初期設定の Privacy Manager の証明書をいつも使用する必要はありません。Privacy Manager のさまざまな機能によって、使用する Privacy Manager の証明書を選択できます。

Privacy Manager の証明書の削除

Privacy Manager の証明書を削除すると、この証明書で暗号化したファイルを開いたり、データを表示したりすることができなくなります。間違えて Privacy Manager の証明書を削除した場合は、証明書のインストール時に作成したバックアップ ファイルを使用して証明書を復元できます。

Privacy Manager の証明書を削除するには、以下の操作を行います。

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**証明書マネージャー**]をクリックします。
2. 削除する Privacy Manager の証明書をクリックしてから、[**詳細**]をクリックします。
3. [**削除**]をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。
5. [**閉じる**]をクリックし、[**適用**]をクリックします。

Privacy Manager の証明書の復元

間違えて Privacy Manager の証明書を削除した場合は、証明書のインストールまたはエクスポート時に作成したバックアップ ファイルを使用して証明書を復元できます。

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**移行**]をクリックします。
2. [**復元**]ボタンをクリックします。
3. [移行ファイル]ページで[**参照**]をクリックし、Privacy Manager の証明書のインストールまたはエクスポートの際に作成した.dppsm ファイルを探してから、[**次へ**]をクリックします。
4. [移行ファイルをインポートしました]ページで、[**完了**]をクリックします。
5. [**閉じる**]をクリックし、[**適用**]をクリックします。

注記： 詳しくは、「Privacy Manager の証明書のインストール」または「Privacy Manager の証明書および信頼済み連絡先のエクスポート」を参照してください。

Privacy Manager の証明書の廃止

お使いの Privacy Manager の証明書のセキュリティに問題があると感じる場合、その証明書を廃止できます。

注記： Privacy Manager の証明書を廃止しても、削除はされません。この証明書は、暗号化したファイルを表示するために引き続き使用できます。

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**証明書マネージャー**]をクリックします。
2. [**詳細設定**]をクリックします。
3. 廃止する Privacy Manager の証明書をクリックしてから、[**廃止**]をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

5. 選択したセキュリティ ログイン方法で認証します。

6. 画面の説明に沿って操作します。

信頼済み連絡先の管理

信頼済み連絡先とは、安全に通信ができるように、互いに Privacy Manager の証明書を交換したユーザーのことです。

信頼済み連絡先の追加

1. 信頼済み連絡先の受信者に、電子メールで招待状を送信します。

2. 信頼済み連絡先の受信者が、この電子メールに返信します。

3. 信頼済み連絡先の受信者から返信メールを受け取ったら、[**承認**]をクリックします。

信頼済み連絡先の電子メール招待状は、個々の受信者宛てに送信することも、Microsoft Outlook のアドレス帳に記載されているすべての連絡先に送信することもできます。

注記： 信頼済み連絡先になるための招待状に返信するには、信頼済み連絡先の受信者のコンピューターに、Privacy Manager または別のクライアントがインストールされている必要があります。別のクライアントのインストールについて詳しくは、DigitalPersona の Web サイト http://DigitalPersona.com/PrivacyManager/（英語サイト）を参照してください。

信頼済み連絡先の追加

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**信頼済み連絡先**]→[**連絡先の招待**]ボタンの順にクリックします。

   または

   Microsoft Outlook で、ツールバーの[**安全に送信**]の横にある下向きの矢印をクリックしてから、[**連絡先の招待**]をクリックします。

2. [証明書の選択]ダイアログ ボックスが表示された場合は、使用する Privacy Manager の証明書をクリックしてから[**OK**]をクリックします。

3. [信頼済み連絡先の招待]ダイアログ ボックスが表示されたら、画面に表示されている内容を確認してから[**OK**]をクリックします。

   電子メールが自動的に生成されます。

4. 信頼済み連絡先に追加する受信者の電子メール アドレスを 1 つ以上入力します。

5. テキストを編集し、自分の名前を署名します（オプション）。

6. [**送信**]をクリックします。

   注記： Privacy Manager の証明書を取得していない場合は、信頼済み連絡先要求の送信に Privacy Manager の証明書が必要であることを知らせるメッセージが表示されます。[OK]をクリックして、証明書の要求ウィザードを起動します。

7. 選択したセキュリティ ログイン方法で認証します。

8. 信頼済み連絡先になるための招待を承認した返信メールを受信者から受け取ったら、電子メール右下隅の[承認]をクリックします。

ダイアログ ボックスが開き、受信者が信頼済み連絡先の一覧に正常に追加されたことを確認できます。

9. [**OK**]をクリックします。

Microsoft Outlook のアドレス帳を使用した信頼済み連絡先の追加

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**信頼済み連絡先**]→[**連絡先の招待**]ボタンの順にクリックします。

   または

   Microsoft Outlook で、ツールバーの[**安全に送信**]の横にある下向きの矢印をクリックしてから、[**Outlook のすべての連絡先を招待**]をクリックします。

2. [信頼済み連絡先の招待]ページが開いたら、信頼済み連絡先に追加する受信者の電子メール アドレスを選択してから[**次へ**]をクリックします。

3. [招待状の送信]ページが開いたら、[**完了**]をクリックします。

   選択した Microsoft Outlook の電子メール アドレスを一覧表示した電子メールが自動生成されます。

4. テキストを編集し、自分の名前を署名します（オプション）。

5. [**送信**]をクリックします。

   注記： Privacy Manager の証明書を取得していない場合は、信頼済み連絡先要求の送信に Privacy Manager の証明書が必要であることを知らせるメッセージが表示されます。[**OK**]をクリックして、証明書の要求ウィザードを起動します。

6. 選択したセキュリティ ログイン方法で認証します。

   注記： 信頼済み連絡先の受信者は、電子メールを受信したら、その電子メールを開いて右下隅の[承認]をクリックし、確認用のダイアログ ボックスが表示されたら[OK]をクリックする必要があります。

7. 信頼済み連絡先になるための招待を承認した返信メールを受信者から受け取ったら、電子メール右下隅の[承認]をクリックします。

   ダイアログ ボックスが開き、受信者が信頼済み連絡先の一覧に正常に追加されたことを確認できます。

8. [**OK**]をクリックします。

信頼済み連絡先の詳細の表示

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**信頼済み連絡先マネージャー**]をクリックします。

2. 信頼済み連絡先をクリックします。

3. [**連絡先の詳細**]をクリックします。

4. 詳細の確認を終えたら、[**OK**]をクリックします。

信頼済み連絡先の削除

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**信頼済み連絡先マネージャー**]をクリックします。
2. 削除する信頼済み連絡先をクリックします。
3. [**連絡先の削除**]をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

信頼済み連絡先の廃止状態の確認

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**信頼済み連絡先マネージャー**]をクリックします。
2. [信頼済み連絡先]をクリックします。
3. [**詳細**]ボタンをクリックします。

   [高度な信頼済み連絡先管理]ダイアログ ボックスが開きます。
4. [**廃止の確認**]をクリックします。
5. [**閉じる**]をクリックします。

一般的なタスク

Microsoft Office ドキュメントでの Privacy Manager の使用

Privacy Manager の証明書をインストールすると、Microsoft Office 2007 の Microsoft Word、Microsoft Excel、および Microsoft PowerPoint のすべてのドキュメントで、ツールバーの右側に[署名と暗号化]ボタンが表示されます。

注記： Microsoft Office 2007 をお使いの場合は、すべての Microsoft Update を適用する必要があります。適用しないと、署名付き電子メールの一部が[迷惑メール]フォルダーに保存されてしまいます。

Microsoft Office ドキュメントでの Privacy Manager の設定

1. タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを右クリックし、[**File Sanitizer**]を強調表示してから、[**今すぐシュレッド**]をクリックします。
2. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

または

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**設定**]→[**ドキュメント**]タブの順にクリックします。

   または

   Microsoft Office ドキュメントのツールバーで、[**署名と暗号化**]の横にある下向きの矢印をクリックしてから[**設定**]をクリックします。
2. 設定する操作を選択して、[**OK**]をクリックします。

Microsoft Office ドキュメントへの署名

1. Microsoft Word、Microsoft Excel、または Microsoft PowerPoint でドキュメントを作成し、保存します。
2. [**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**ドキュメントへの署名**]をクリックします。
3. 選択したセキュリティ ログイン方法で認証します。
4. 確認用のダイアログ ボックスが表示されたら、画面に表示されている内容を確認してから[**OK**]をクリックします。

後でドキュメントを編集する場合は、以下の操作を行います。

1. 画面の左上隅にある[**Office**]ボタンをクリックします。
2. [**準備**]→[**最終版としてマーク**]の順にクリックします。
3. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックして作業を続けます。
4. 編集が終わったら、再びドキュメントに署名します。

Microsoft Word または Microsoft Excel ドキュメント署名時の署名欄の追加

Privacy Manager では、Microsoft Word または Microsoft Excel ドキュメントに署名する際に署名欄を追加できます。

1. Microsoft Word または Microsoft Excel でドキュメントを作成し、保存します。
2. [**ホーム**]メニューをクリックします。
3. [**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**署名の前に署名欄を追加**]をクリックします。

   注記： このオプションを選択すると、[署名の前に署名欄を追加]の横にチェック マークが表示されます。初期設定では、このオプションは有効になっています。

4. [**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**ドキュメントへの署名**]をクリックします。
5. 選択したセキュリティ ログイン方法で認証します。

Microsoft Word または Microsoft Excel ドキュメントへの推奨する署名者の追加

推奨する署名者を指名することによって、ドキュメントに複数の署名欄を追加できます。推奨する署名者とは、ドキュメントに署名欄を追加するために Microsoft Word または Microsoft Excel ドキュメントの所有者が指名したユーザーのことです。推奨する署名者には自分自身を指名することも、別の人物を指名してドキュメントへの署名を依頼することもできます。たとえば、部署内の全員の署名が必要なドキュメントを準備する場合、特定の日付で署名するよう指示した全員分の署名欄を、ドキュメントの最終ページの最下部に設けることができます。

推奨する署名者を Microsoft Word または Microsoft Excel ドキュメントに追加するには、以下の操作を行います。

1. Microsoft Word または Microsoft Excel でドキュメントを作成し、保存します。
2. [**挿入**]メニューをクリックします。

3. ツールバーの[**テキスト**]グループで、[**署名欄**]の横にある矢印をクリックしてから[**Privacy Manager 署名プロバイダー**]をクリックします。

   [署名の設定]ダイアログ ボックスが表示されます。

4. ボックス内の[**推奨する署名者**]の下に、推奨する署名者を入力します。

5. ボックス内の[**署名者への指示**]の下に、この推奨する署名者へのメッセージを入力します。

   注記： このメッセージはタイトルとして表示されますが、ドキュメントに署名すると、削除したりユーザーのタイトルに置き換えたりすることができます。

6. [**署名欄に署名日を表示**]チェック ボックスにチェックを入れて、日付を表示します。

7. [**署名欄に署名者のタイトルを表示**]チェック ボックスにチェックを入れて、タイトルを表示します。

   注記： ドキュメントの所有者が、推奨する署名者を自身のドキュメントに割り当てているために、[**署名欄に署名日を表示**]および[**署名欄に署名者のタイトルを表示**]の各チェック ボックスにチェックが入っていない場合は、その推奨された署名者は署名欄に日付やタイトルを表示できません。これには、その推奨された署名者のドキュメント設定は関係しません。

8. [**OK**]をクリックします。

推奨する署名者の署名欄の追加

推奨する署名者がドキュメントを開くと、自分の名前が角かっこで囲まれて表示され、署名を求められていることがわかります。

ドキュメントに署名するには、以下の操作を行います。

1. 適切な署名欄をダブルクリックします。

2. 選択したセキュリティ ログイン方法で認証します。

   ドキュメントの所有者が指定した設定に従って、署名欄が表示されます。

Microsoft Office ドキュメントの暗号化

自分自身と信頼済み連絡先のために、Microsoft Office ドキュメントを暗号化できます。ドキュメントを暗号化してから閉じると、自分自身と一覧から選択した信頼済み連絡先は、このドキュメントを開く際に認証が必要となります。

Microsoft Office ドキュメントを暗号化するには、以下の操作を行います。

1. Microsoft Word、Microsoft Excel、または Microsoft PowerPoint でドキュメントを作成し、保存します。

2. [**ホーム**]メニューをクリックします。

3. [**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**ドキュメントの暗号化**]をクリックします。

   [信頼済み連絡先の選択]ダイアログ ボックスが表示されます。

4. ドキュメントを開いて内容を閲覧できるようにする信頼済み連絡先の名前をクリックします。

   注記： 信頼済み連絡先の名前を複数選択するには、Ctrl キーを押しながら個々の名前をクリックします。

5. [**OK**]をクリックします。

6. 選択したセキュリティ ログイン方法で認証します。

後でドキュメントを編集する場合は、「Microsoft Office ドキュメントへの署名」に記載されている操作を行います。暗号化を解除すると、ドキュメントを編集できます。再びドキュメントを暗号化するには、ここに記載されている操作を行います。

Microsoft Office ドキュメントの暗号化の解除

Microsoft Office ドキュメントの暗号化を解除すると、自分自身と信頼済み連絡先は、認証なしでこのドキュメントを開いて内容を閲覧できるようになります。

Microsoft Office ドキュメントの暗号化を解除するには、以下の操作を行います。

1. 暗号化された Microsoft Word、Microsoft Excel、または Microsoft PowerPoint ドキュメントを開きます。

2. 選択したセキュリティ ログイン方法で認証します。

3. [**ホーム**]メニューをクリックします。

4. [**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**暗号化の解除**]をクリックします。

暗号化された Microsoft Office ドキュメントの送信

電子メール メッセージに、暗号化された Microsoft Office ドキュメントを添付できます。電子メール自体への署名や暗号化は不要です。これを行うには、ファイルを添付した一般の電子メールの場合と同様に、署名または暗号化したドキュメントを添付した電子メールを作成して、送信します。

ただし、最適なセキュリティのため、署名または暗号化された Microsoft Office ドキュメントを添付する場合は、電子メールを暗号化することをおすすめします。

署名および暗号化した Microsoft Office ドキュメントを添付して、封印した電子メールを送信するには、以下の操作を行います。

1. Microsoft Outlook で、[**新規作成**]または[**返信**]をクリックします。

2. 電子メール メッセージを入力します。

3. Microsoft Office ドキュメントを添付します。

4. 詳しい手順については、「電子メール メッセージの封印および送信」を参照してください。

署名付き Microsoft Office ドキュメントの表示

注記： 署名付き Microsoft Office ドキュメントを表示するには、Privacy Manager の証明書は不要です。

署名付き Microsoft Office ドキュメントを開くと、ドキュメントの横に[署名]ダイアログ ボックスが開き、ドキュメントに署名したユーザーの名前と署名日が表示されます。名前を右クリックすると、詳細を確認できます。

暗号化された Microsoft Office ドキュメントの表示

暗号化された Microsoft Office ドキュメントを別のコンピューターから閲覧するには、そのコンピューターに Privacy Manager をインストールしておく必要があります。また、ファイルの暗号化に使用した Privacy Manager の証明書をインポートする必要があります。

暗号化された Microsoft Office ドキュメントを信頼済み連絡先が閲覧するには、Privacy Manager の証明書が必要になるため、信頼済み連絡先のコンピューターに Privacy Manager をインストールしておく必要があります。また、暗号化された Microsoft Office ドキュメントの所有者が、この信頼済み連絡先を選択している必要があります。

Microsoft Outlook での Privacy Manager の使用

Privacy Manager をインストールすると、Microsoft Outlook のツールバーに[プライバシ]ボタンが表示されるようになります。また、Microsoft Outlook の各電子メール メッセージのツール バーに[安全に送信]ボタンが表示されるようになります。

注記： Microsoft Office 2007 をお使いの場合は、すべての Microsoft Update を適用する必要があります。適用しないと、署名付き電子メールの一部が[迷惑メール]フォルダーに保存されてしまいます。

Microsoft Outlook 用の Privacy Manager の設定

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**設定**]→[**電子メール**]タブの順にクリックします。

   または

   Microsoft Outlook のメインのツールバーで、[**プライバシ**]の横にある下向きの矢印をクリックしてから[**設定**]をクリックします。

   または

   Microsoft の電子メール メッセージのツールバーで、[**安全に送信**]の横にある下向きの矢印をクリックしてから[**設定**]をクリックします。

2. 安全な電子メールを送信するときに実行する操作を選択し、[**OK**]をクリックします。

電子メール メッセージの署名および送信

1. Microsoft Outlook で、[**新規作成**]または[**返信**]をクリックします。
2. 電子メール メッセージを入力します。
3. [**安全に送信**]の横にある下向きの矢印をクリックしてから、[**署名して送信**]をクリックします。
4. 選択したセキュリティ ログイン方法で認証します。

電子メール メッセージの封印および送信

デジタル処理によって署名および封印（暗号化）されている封印済み電子メールを閲覧できるのは、信頼済み連絡先の一覧から選択したユーザーのみです。

電子メールを封印して信頼済み連絡先に送信するには、以下の操作を行います。

1. Microsoft Outlook で、[**新規作成**]または[**返信**]をクリックします。
2. 電子メール メッセージを入力します。
3. [**安全に送信**]の横にある下向きの矢印をクリックしてから、[**信頼済み連絡先宛てに封印して送信**]をクリックします。
4. 選択したセキュリティ ログイン方法で認証します。

封印された電子メール メッセージの表示

封印された電子メール メッセージを開くと、電子メールの見出しにセキュリティ ラベルが表示されます。このセキュリティ ラベルには、以下の情報が記載されています。

- 電子メールに署名した人物の身元確認に使用された証明書
- 電子メールに署名した人物の証明書の確認に使用された製品

高度なタスク

別のコンピューターへの Privacy Manager の証明書と信頼済み連絡先の移行

Privacy Manager の証明書および信頼済み連絡先を、別のコンピューターに安全に移行できます。これには、Privacy Manager の証明書および信頼済み連絡先をパスワードで保護されたファイルとしてネットワーク上の場所かリムーバブル ストレージ デバイスにエクスポートしてから、新しいコンピューターにこのファイルをインポートします。

Privacy Manager の証明書および信頼済み連絡先のエクスポート

Privacy Manager の証明書および信頼済み連絡先をパスワードで保護されたファイルにエクスポートするには、以下の操作を行います。

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**移行**]をクリックします。
2. [**移行ファイルのエクスポート**]をクリックします。
3. [データの選択]ページで、移行ファイルに含めるデータのカテゴリを選択してから[**次へ**]をクリックします。
4. [移行ファイル]ページで、ファイル名を入力するか[**参照**]をクリックして場所を探し、[**次へ**]をクリックします。
5. パスワードの入力と確認を行い、[**次へ**]をクリックします。

   注記： このパスワードは、移行ファイルをインポートするときに必要となるため、安全な場所に保管してください。

6. 選択したセキュリティ ログイン方法で認証します。
7. [移行ファイルを保存しました]ページで、[**完了**]をクリックします。

Privacy Manager の証明書および信頼済み連絡先のインポート

Privacy Manager の証明書および信頼済み連絡先をパスワードで保護されたファイルにインポートするには、以下の操作を行います。

1. Security Manager の左側のパネルで、[**Privacy Manager**]を展開して、[**移行**]をクリックします。
2. [**移行ファイルのインポート**]をクリックします。
3. [データの選択]ページで、移行ファイルに含めるデータのカテゴリを選択してから[**次へ**]をクリックします。

4. [移行ファイル]ページで、ファイル名を入力するか[**参照**]をクリックして場所を探し、[**次へ**]をクリックします。

5. [移行ファイルのインポート]ページで、[**完了**]をクリックします。

7　File Sanitizer for HP ProtectTools

File Sanitizer は、コンピューター上の重要なファイルやフォルダー（個人情報や個人ファイル、履歴データや Web 関連データ、その他のデータ コンポーネント）を安全に消去したり、ハードディスク ドライブを定期的にブリーチしたりすることができるツールです。

注記： File Sanitizer は現在、ハードディスク ドライブ上でのみ動作します。

シュレッドについて

Windows でファイルやフォルダーを削除しても、そのファイルやフォルダーの内容はハードディスク ドライブから完全に削除されるわけではありません。Windows はファイルやフォルダーの参照情報のみを削除します。他のファイルやフォルダーによってハードディスク ドライブの同じ領域を新しい情報で上書きしないかぎり、ファイルやフォルダーの内容はハードディスク ドライブに引き続き残ったままとなります。

ファイルやフォルダーのシュレッドは、データの内容をわからなくするアルゴリズムが実行されて元のファイルやフォルダーを取り戻すことが事実上不可能になる点で、通常の Windows の削除（File Sanitizer ではシンプル削除とも言います）とは異なります。

シュレッド プロファイル（[セキュリティ設定、高]、[セキュリティ設定、中]、または[セキュリティ設定、低]）を選択すると、あらかじめ定義されているファイルやフォルダーの一覧と消去方法がシュレッドのために自動で選択されます。また、シュレッド プロファイルをカスタマイズして、シュレッド サイクル数、シュレッド対象に含めるファイルやフォルダー、シュレッド前に確認するファイルやフォルダー、およびシュレッド対象から除外するファイルやフォルダーを指定することもできます。

自動シュレッドのスケジュールを設定することができます。また、必要に応じていつでもファイルやフォルダーを手動シュレッドすることもできます。

空き領域ブリーチについて

空き領域ブリーチを実行すると、削除されたファイルやフォルダーに対してランダムなデータを安全に上書きできるため、削除されたファイルやフォルダーの元の内容をユーザーは参照できなくなります。

注記： 空き領域ブリーチは、Windows のゴミ箱を使用して削除したファイルやフォルダー、または手動で削除したファイルやフォルダーを対象とする機能です。空き領域ブリーチを実行しても、シュレッドされたファイルやフォルダーにセキュリティが追加されることはありません。

タスクバーの右端の通知領域にある[HP ProtectTools]アイコンを使用して、空き領域ブリーチの自動スケジュールを有効にするか、空き領域ブリーチを手動で実行することができます。

セットアップ手順

File Sanitizer の起動

File Sanitizer を起動するには、以下の操作を行います。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。
2. Security Manager の左側のパネルで、[**File Sanitizer**]をクリックします。

または

- [**File Sanitizer**]アイコンをダブルクリックします。

または

- タスクバーの右端の通知領域にある[HP ProtectTools]アイコンを右クリックし、[**File Sanitizer**]を強調表示してから、[**File Sanitizer を開く**]をクリックします。

空き領域ブリーチのスケジュール設定

注記： 空き領域ブリーチは、Windows のゴミ箱を使用して削除したファイルやフォルダー、または手動で削除したファイルやフォルダーを対象とする機能です。空き領域ブリーチを実行しても、シュレッドされたファイルやフォルダーにセキュリティが追加されることはありません。

空き領域ブリーチのスケジュールを設定するには、以下の操作を行います。

1. Security Manager の左側のパネルで、[**File Sanitizer**]を展開して、[**ブリーチ**]をクリックします。
2. [**スケジューラの起動**]チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、ハードディスク ドライブをブリーチする日付と時刻を入力します。
3. [**保存**]アイコンをクリックします。

   注記： 空き領域ブリーチ操作は、長い時間がかかる場合があります。空き領域ブリーチはバックグラウンドで実行されますが、プロセッサの使用量が大きくなるため、コンピューターの動作が遅くなる場合があります。

シュレッド スケジュールの設定

1. Security Manager の左側のパネルで、[**File Sanitizer**]を展開して、[**シュレッド**]をクリックします。
2. シュレッド オプションを以下の中から選択します。
   - [**Windows のシャットダウン時**]：選択されているすべてのファイルやフォルダーを Windows のシャットダウン時にシュレッドするには、このオプションを選択します。

     注記： このオプションを選択すると、シャットダウン時にダイアログ ボックスが表示され、選択されているファイルやフォルダーのシュレッドを実行するか、シュレッド処理を中止するかを確認するメッセージが表示されます。シュレッド処理に進む場合は[はい]、シュレッドを中止する場合は[いいえ]をクリックします。Windows では、シャットダウンに備えてソフトウェアが終了され、エラーが生成されるため、[はい]または[いいえ]オプションの選択はすぐに行う必要があります。シュレッド処理に進むために[いいえ]を選択すると、File Sanitizer が応答していないことを示すエラー画面が Windows によって表示されることがあります。File Sanitizer がシュレッド処理を完了できるようにしてから、もう一度シャットダウンを開始します。
   - [**Web ブラウザーの起動時**]：ブラウザーの URL 履歴など、選択されているすべての Windows 関連ファイルやフォルダーを Web ブラウザーの起動時にシュレッドするには、このオプションを選択します。
   - [**Web ブラウザーの終了時**]：ブラウザーの URL 履歴など、選択されているすべての Windows 関連ファイルやフォルダーを Web ブラウザーの終了時にシュレッドするには、このオプションを選択します。
   - [**キーの組み合わせ**]：キーの組み合わせでシュレッドを開始するには、このオプションを選択します。
   - [**スケジューラ**]：[スケジューラの起動]チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、選択されているファイルやフォルダーをシュレッドする日付と時刻を入力します。
3. [**保存**]アイコンをクリックします。

シュレッド プロファイルの選択または作成

あらかじめ定義されているプロファイルを選択するか、自分のプロファイルを作成して、消去方法を指定したりシュレッドするファイルやフォルダーを選択したりすることができます。

あらかじめ定義されているシュレッド プロファイルの選択

あらかじめ定義されているシュレッド プロファイル（[セキュリティ設定、高]、[セキュリティ設定、中]、または[セキュリティ設定、低]）を選択すると、あらかじめ定義されている消去方法とファイルやフォルダーの一覧が自動的に選択されます。[詳細を表示]ボタンをクリックすると、シュレッド用に選択されているファイルやフォルダーのあらかじめ定義されている一覧が表示されます。

あらかじめ定義されているシュレッド プロファイルを選択するには、以下の操作を行います。

1. Security Manager の左側のパネルで、[**File Sanitizer**]を展開して、[**設定**]をクリックします。
2. あらかじめ定義されているシュレッド プロファイルをクリックします。
3. [**詳細を表示**]をクリックして、シュレッド用に選択されているファイルやフォルダーの一覧を表示します。
4. [**次のフォルダー/ファイルをシュレッドする**]で、シュレッド前に確認する各ファイルやフォルダーの横のチェック ボックスにチェックを入れます。
5. [**適用**]をクリックします。

高度にセキュリティ設定されたシュレッド プロファイルのカスタマイズ

シュレッド プロファイルを作成するには、シュレッド サイクル数、シュレッド対象に含めるファイルやフォルダー、シュレッド前に確認するファイルやフォルダー、およびシュレッド対象から除外するファイルやフォルダーを指定します。

1. Security Manager の左側のパネルで、[**File Sanitizer**]を展開して[**設定**]をクリックし、[**高度なセキュリティ設定**]を選択してから、[**詳細の表示**]をクリックします。
2. シュレッド サイクル数を指定します。

   注記： 各ファイルやフォルダーに対して、指定した数のシュレッド サイクルが実行されます。たとえば、シュレッド サイクルで 3 を選択すると、データの内容をわからなくするアルゴリズムが異なる 3 つの時間に実行されます。高いセキュリティ設定でシュレッド サイクルを選択すると、シュレッドに非常に長い時間がかかる場合があります。ただし、指定するシュレッド サイクル数を大きくするほど、コンピューターのセキュリティは高まります。

3. シュレッドするファイルやフォルダーを選択するには、以下の操作を行います。
   a. [**使用できるシュレッド オプション**]で、ファイルやフォルダーをクリックしてから[**追加**]をクリックします。
   b. カスタム ファイルやフォルダーを追加するには、[**カスタム オプションの追加**]をクリックし、ファイル名またはフォルダー名を入力して[**OK**]をクリックします。カスタム ファイルやフォルダーをクリックして、[**追加**]をクリックします。

      注記： 使用できるシュレッド オプションからファイルやフォルダーを削除するには、ファイルやフォルダーをクリックしてから[**削除**]をクリックします。

4. [**次のフォルダー/ファイルをシュレッドする**]で、シュレッド前に確認する各ファイルやフォルダーの横のチェック ボックスにチェックを入れます。

   注記： シュレッド リストからファイルやフォルダーを削除するには、ファイルやフォルダーをクリックしてから[**削除**]をクリックします。

5. [**次のフォルダー/ファイルをシュレッドしない**]で、[**追加**]をクリックして、シュレッド対象から除外するファイルやフォルダーを指定します。

6. シュレッド プロファイルの設定を完了したら、[**適用**]をクリックします。

シンプル削除プロファイルのカスタマイズ

シンプル削除プロファイルは、シュレッドではなく、標準的なファイルやフォルダーの削除を実行します。シンプル削除プロファイルをカスタマイズするには、シンプル削除対象に含めるファイルやフォルダー、シンプル削除の実行前に確認するファイルやフォルダー、およびシンプル削除対象から除外するファイルやフォルダーを指定します。

注記： シンプル削除オプションを使用する場合は、空き領域ブリーチを定期的に実行することを強くおすすめします。

1. Security Manager の左側のパネルで、[**File Sanitizer**]を展開して[**設定**]をクリックし、[**シンプル削除設定**]を選択してから、[**詳細の表示**]をクリックします。

2. 削除するファイルやフォルダーを選択するには、以下の操作を行います。

   a. [**使用できる削除オプション**]で、ファイルやフォルダーをクリックしてから[**追加**]をクリックします。

   b. カスタム ファイルやフォルダーを追加するには、[**カスタム オプションの追加**]をクリックし、ファイル名またはフォルダー名を入力して[**OK**]をクリックします。カスタム ファイルやフォルダーをクリックして、[**追加**]をクリックします。

   注記： 使用できる削除オプションからファイルやフォルダーを削除するには、ファイルやフォルダーをクリックしてから[**削除**]をクリックします。

3. [**次のフォルダー/ファイルを削除する**]で、削除前に確認する各ファイルやフォルダーの横のチェック ボックスにチェックを入れます。

   注記： 削除リストからファイルやフォルダーを削除するには、ファイルやフォルダーをクリックしてから[**削除**]をクリックします。

4. [**次のフォルダー/ファイルを削除しない**]で、[**追加**]をクリックして、削除対象から除外するファイルやフォルダーを指定します。

5. シンプル削除プロファイルの設定を完了したら、[**適用**]をクリックします。

一般的なタスク

キーの組み合わせによるシュレッドの開始

キーの組み合わせを指定するには、以下の操作を行います。

1. Security Manager の左側のパネルで、[**File Sanitizer**]を展開して、[**シュレッド**]をクリックします。
2. [**キーの組み合わせ**]チェック ボックスにチェックを入れます。
3. 使用できるボックスに文字を 1 つ入力してから、[**CTRL**]ボックス、[**ALT**]ボックス、[**SHIFT**]ボックスのどれかまたは 3 つすべてにチェックを入れます。

   たとえば、S キーと Ctrl + Shift キーを使用して自動シュレッドを開始するには、ボックスに S と入力してから、[**CTRL**]オプションと[**SHIFT**]オプションにチェックを入れます。

注記：　設定済みの他のキーの組み合わせとは異なるキーの組み合わせを選択してください。

キーの組み合わせでシュレッドを開始するには、以下の操作を行います。

1. 選択した文字を押しながら、Ctrl + Alt キーまたは Shift キー（またはあらかじめ指定した組み合わせのキー）を押します。
2. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

[File Sanitizer]アイコンの使用

△ 注意：　シュレッドしたファイルやフォルダーは復元できません。手動でシュレッドするために選択するファイルやフォルダーについては、十分に検討してください。

1. シュレッドするドキュメントまたはフォルダーに移動します。
2. シュレッドするファイルやフォルダーをデスクトップの[File Sanitizer]アイコンにドラッグします。
3. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

単一のファイルやフォルダーの手動シュレッド

△ 注意：　シュレッドしたファイルやフォルダーは復元できません。手動でシュレッドするために選択するファイルやフォルダーについては、十分に検討してください。

1. タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを右クリックし、[**File Sanitizer**]を強調表示してから、[**単一フォルダー/ファイルをシュレッド**]をクリックします。
2. [参照]ダイアログ ボックスが開いたら、シュレッドするファイルやフォルダーに移動してから[**開く**]をクリックします。

   注記：　選択できるファイルやフォルダーは、単一のファイルまたはフォルダーです。

3. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

または

1. デスクトップにある[**File Sanitizer**]アイコンを右クリックしてから、[**単一フォルダー/ファイルをシュレッド**]をクリックします。
2. [参照]ダイアログ ボックスが開いたら、シュレッドするファイルやフォルダーに移動してから[**OK**]をクリックします。
3. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

または

1. Security Manager の左側のパネルで、[**File Sanitizer**]を展開して、[**シュレッド**]をクリックします。
2. [**参照**]ボタンをクリックします。
3. [参照]ダイアログ ボックスが開いたら、シュレッドするファイルやフォルダーに移動してから[**開く**]をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

選択されているすべてのファイルやフォルダーの手動シュレッド

1. タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを右クリックし、[**File Sanitizer**]を強調表示してから、[**今すぐシュレッド**]をクリックします。
2. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

または

1. デスクトップにある[**File Sanitizer**]アイコンを右クリックしてから、[**今すぐシュレッド**]をクリックします。
2. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

空き領域ブリーチの手動実行

1. タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを右クリックし、[**File Sanitizer**]を強調表示してから、[**今すぐブリーチ**]をクリックします。
2. ブリーチ操作が始まったことを確認する通知メッセージが表示されます。

または

1. Security Manager の左側のパネルで、[**File Sanitizer**]を展開して、[**ブリーチ**]をクリックします。
2. [**今すぐブリーチ**]をクリックします。
3. ブリーチ操作が始まったことを確認する通知メッセージが表示されます。

シュレッド操作または空き領域ブリーチ操作の停止

シュレッド操作または空き領域ブリーチ操作の実行中は、通知領域にある[HP ProtectTools Security Manager]アイコンの上にメッセージが表示されます。このメッセージには、シュレッドまたは空き領域ブリーチの進行状況の詳細（完了した割合）と、操作を停止するためのオプションが表示されます。

この操作を停止するには、以下の操作を行います。

▲ メッセージをクリックしてから[**停止**]ボタンをクリックすると、操作がキャンセルされます。

ログ ファイルの表示

シュレッド操作または空き領域ブリーチ操作を実行するたびに、エラーのログ ファイルまたは障害のログ ファイルが生成されますこれらのログ ファイルは、最新のシュレッド操作または空き領域ブリーチ操作に従って常に更新されます。

注記： 正常にシュレッドまたはブリーチされたファイルは、ログ ファイルには表示されません。

ログ ファイルには、シュレッド操作について作成されるファイルと空き領域ブリーチ操作について作成されるファイルがあります。どちらのファイルも、ハードディスク ドライブ上の以下の場所に存在します。

- C:¥Program Files¥Hewlett-Packard¥File Sanitizer¥[Username]_ShredderLog.txt
- C:¥Program Files¥Hewlett-Packard¥File Sanitizer¥[Username]_DiskBleachLog.txt

8 Embedded Security for HP ProtectTools

注記： Embedded Security for HP ProtectTools を使用するには、統合された TPM（Trusted Platform Module）セキュリティ チップがコンピューターに内蔵されている必要があります。ほとんどの企業向け HP 製デスクトップ コンピューターには、情報セキュリティ国際評価基準（Common Criteria）による認定を受け、TCG 仕様に適合する唯一のチップである Infineon TPM が内蔵されています。

Embedded Security for HP ProtectTools は、ユーザー データや証明情報を不正なアクセスから保護します。このソフトウェア モジュールには、以下のセキュリティ機能があります。

- 高度な Microsoft EFS（Encrypting File System）ファイルおよびフォルダーの暗号化（EFS は Windows Home Edition では利用できません）
- ユーザー データを保護するための PSD（Personal Secure Drive）の作成
- データ管理機能（キー階層のバックアップや復元など）
- Embedded Security ソフトウェアの使用時にデジタル証明書の操作を保護するための他社製アプリケーション（Microsoft Outlook や Internet Explorer など）のサポート

TPM 内蔵セキュリティ チップを使用すると、HP ProtectTools Security Manager の他のセキュリティ機能を強化したり有効にしたりできます。たとえば、Drive Encryption for HP ProtectTools では、内蔵チップを Windows へのログオン時の認証要素として使用できます。

セットアップ手順

△ **注意：** セキュリティ上の危険にさらされないようにするために、IT 管理者が内蔵セキュリティ チップをただちに初期化することを強くおすすめします。内蔵セキュリティ チップを初期化しない場合、不正なユーザー、コンピューター ワーム、またはウィルスがコンピューターのオーナシップを奪い、緊急リカバリ アーカイブの処理やユーザー アクセスの設定など所有者のタスクを制御してしまう可能性があります。

以下の 2 つの項目の手順に沿って操作し、内蔵セキュリティ チップを有効にして初期化します。

Embedded Security for HP ProtectTools のインストール（必要な場合）

Embedded Security for HP ProtectTools をインストールするには、以下の操作を行います。

1. ［スタート］→［すべてのプログラム］→［**Install Embedded Security for HP ProtectTools**］（Embedded Security for HP ProtectTools のインストール）の順にクリックします。
2. ユーザー アカウント制御の警告が表示されたら、［**許可**］をクリックします。
3. ［**次へ**］をクリックし、必要に応じてユーザー名と組織名を入力します。
4. ［**次へ**］→［**インストール**］の順にクリックし、インストールが完了したら［**完了**］をクリックします。
5. 再起動を要求されたら、［**はい**］または［**いいえ**］を選択します。

コンピューター セットアップ（F10）ユーティリティでの内蔵セキュリティ チップの有効化

内蔵セキュリティ チップは、以下で説明する手順に沿って、[Quick Initialization Wizard]（クイック インストール ウィザード）または[コンピューター セットアップ（F10）ユーティリティ]で有効にする必要があります。

コンピューター セットアップ（F10）ユーティリティで内蔵セキュリティ チップを有効にするには、以下の操作を行います。

1. コンピューターの電源を入れるか再起動し、画面の左下隅に[F10=ROM Based Setup]というメッセージが表示されている間に F10 キーを押して、コンピューター セットアップ（F10）ユーティリティを起動します。
2. 管理者パスワードを設定していない場合は、矢印キーを使用して［**Security**］（セキュリティ）→［**Setup password**］（セットアップ パスワード）の順に選択して、Enter キーを押します。
3. ［**New password**］（新しいパスワード）ボックスと［**Verify Password**］（パスワードの確認）ボックスにパスワードを入力して確定します。
4. ［**Security**］メニューで、矢印キーを使用して［**TPM Embedded Security**］（TPM 内蔵セキュリティ）を選択し、Enter キーを押します。
5. ［**Embedded security device state**］（内蔵セキュリティ デバイスの状態）を選択し、［**Enable**］（有効にする）に変更します。

6. F10 キーを押して、Embedded Security の設定への変更を確定します。

7. 設定を保存してコンピュータ セットアップ（F10）ユーティリティを終了するには、矢印キーを使用して［**File**］（ファイル）を選択し、［**Save Changes and Exit**］（変更を保存して終了）をクリックします。次に、画面の説明に沿って操作します。

内蔵セキュリティ チップの初期化

内蔵セキュリティの初期化プロセスでは、以下のタスクを実行します。

- 内蔵セキュリティ チップの所有者のパスワードを設定します。これによって、内蔵セキュリティ チップ上のすべての所有者機能へのアクセスが保護されます。
- 緊急リカバリ アーカイブをセットアップします。緊急リカバリ アーカイブとは、すべてのユーザーの基本ユーザー キーを再暗号化できるようにするための保護された記憶領域です。

内蔵セキュリティ チップを初期化するには、以下の操作を行います。

1. タスク バーの右端の通知領域にある[HP ProtectTools Security Manager]アイコンを右クリックして、［**内蔵セキュリティの初期化**］を選択します。

   HP ProtectTools Embedded Security 初期化ウィザードが起動します。

2. 画面の説明に沿って操作します。

基本ユーザー アカウントのセットアップ

Embedded Security で基本ユーザー アカウントをセットアップすると、以下のタスクが実行されます。

- 暗号化された情報を保護するための基本ユーザー キーが生成され、その基本ユーザー キーを保護するための基本ユーザー キーのパスワードが設定されます。
- 暗号化されたファイルおよびフォルダーを格納するための PSD（Personal Secure Drive）が設定されます。

△ **注意：** 基本ユーザー キーのパスワードは、大切に保管しておいてください。このパスワードがないと、暗号化されたデータにアクセスしたり、暗号化されたデータを復元したりできなくなります。

基本ユーザー アカウントをセットアップしてユーザー セキュリティ機能を有効にするには、以下の操作を行います。

1. Embedded Security ユーザー初期化ウィザードが起動していない場合は、［**スタート**］→［**すべてのプログラム**］→［**HP**］→［**HP ProtectTools Security Manager**］の順にクリックします。

2. 左側のパネルで、［**内蔵セキュリティ**］→［**ユーザーの設定**］の順にクリックします。

3. 右側のパネルで、［**内蔵セキュリティの機能**］の［**設定**］をクリックします。

   [Embedded Security ユーザー初期化ウィザード]が起動します。

4. 画面の説明に沿って操作します。

   注記： セキュリティ保護された電子メールを使用するには、最初に、Embedded Security で作成されたデジタル証明情報を使用するように電子メール クライアントを設定する必要があります。デジタル証明情報が使用できない場合は、証明機関から取得する必要があります。電子メールを設定してデジタル証明情報を取得する手順については、電子メール クライアント ソフトウェアのヘルプを参照してください。

一般的なタスク

基本ユーザー アカウントのセットアップを完了すると、以下のタスクを実行できます。

- ファイルおよびフォルダーの暗号化
- 暗号化された電子メールの送受信

PSD（Personal Secure Drive）の使用

PSD のセットアップを完了すると、次回のログオンで、基本ユーザー キーのパスワードを入力するよう要求されます。基本ユーザー キーのパスワードを正しく入力すると、Windows のエクスプローラーから直接 PSD にアクセスできます。

ファイルおよびフォルダーの暗号化

暗号化ファイルを操作する場合は、以下の規則を考慮してください。

- 暗号化できるファイルおよびフォルダーは、NTFS パーティション上のもののみです。FAT パーティション上のファイルおよびフォルダーは暗号化できません。
- システム ファイルや圧縮されたファイルは暗号化できません。また、暗号化されたファイルは圧縮できません。
- 一時フォルダーは、ハッカーの関心を引く可能性があるため、暗号化するようにしてください。
- ファイルまたはフォルダーを初めて暗号化すると、回復ポリシーが自動的にセットアップされます。暗号化証明情報や秘密キーをなくした場合でも、このポリシーによって、回復エージェントを使用して情報の暗号化を解除できるようになります。

注記： ファイルおよびフォルダーの暗号化は、Windows Home Edition ではサポートされていません。

ファイルおよびフォルダーを暗号化するには、以下の操作を行います。

1. 暗号化するファイルまたはフォルダーを右クリックします。
2. ［**暗号化**］をクリックします。
3. 以下のオプションのどちらかをクリックします。
   - ［**このフォルダーのみに変更を適用する**］
   - ［**このフォルダー、およびサブフォルダーとファイルに変更を適用する**］
4. ［**OK**］をクリックします。

暗号化された電子メールの送受信

Embedded Security では、暗号化された電子メールの送受信を行うことができますが、その手順は電子メールのアクセスに使用しているプログラムによって異なります。詳しくは、Embedded Security ソフトウェアのヘルプおよび使用している電子メール アプリケーション ソフトウェアのヘルプを参照してください。

高度なタスク

バックアップおよび復元

Embedded Security のバックアップ機能では、緊急の場合に復元される証明情報を含むアーカイブが作成されます。

バックアップ ファイルの作成

バックアップ ファイルを作成するには、以下の操作を行います。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。
2. 左側のパネルで、[**内蔵セキュリティ**]→[**バックアップ**]の順にクリックします。
3. 右側のパネルで、[**設定**]をクリックします。HP Embedded Security for HP ProtectTools バックアップ ウィザードが起動します。
4. 画面の説明に沿って操作します。

バックアップ ファイルからの証明データの復元

バックアップ ファイルからデータを復元するには、以下の操作を行います。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。
2. 左側のパネルで、[**内蔵セキュリティ**]→[**バックアップ**]の順にクリックします。
3. 右側のパネルで、[**すべて復元**]をクリックします。HP Embedded Security for HP ProtectTools バックアップ ウィザードが起動します。
4. 画面の説明に沿って操作します。

所有者のパスワードの変更

所有者のパスワードを変更するには、以下の操作を行います。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。
2. 左側のパネルで、[**内蔵セキュリティ**]→[**アドバンス**]の順にクリックします。
3. 右側のパネルで、[**所有者のパスワード**]の[**変更**]をクリックします。
4. 古い所有者のパスワードを入力した後、新しい所有者のパスワードを設定して確定します。
5. [**OK**]をクリックします。

ユーザー パスワードの再設定

ユーザーが忘れたパスワードを管理者に再設定してもらうことができます。詳しくは、ソフトウェアのヘルプを参照してください。

移行ウィザードによるキーの移行

移行は、キーや証明情報の管理、復元、転送などを行うことができる、高度な管理者タスクです。

移行について詳しくは、Embedded Security ソフトウェアのヘルプを参照してください。

9 Device Access Manager for HP ProtectTools

このセキュリティ ツールは管理者のみが使用できます。Device Access Manager for HP ProtectTools は、コンピューター システムに取り付けられたデバイスを不正なアクセスから保護する以下のセキュリティ機能を備えています。

- デバイス アクセスを定義するためにユーザーごとに作成されるデバイス プロファイル
- グループ メンバーシップに基づいて許可または拒否可能なデバイス アクセス制御

注記： Device Access Manager は、Windows の[ローカル ユーザーとグループ]を使用してアクセスを管理します。Windows Home Edition では、[ローカル ユーザーとグループ]がサポートされていないため、Device Access Manager は正しく機能しません。ただし、Windows Vista の Home Edition では、DOS コマンドを使用してユーザー設定を行うと Device Access Manager が動作します。手順については、Device Access Manager のヘルプファイルを参照してください。

バックグラウンド サービスの開始

デバイス プロファイルを適用するには、HP ProtectTools Device Locking/Auditing（HP ProtectTools デバイス ロック/検査）バックグラウンド サービスを実行している必要があります。最初にデバイス プロファイルを適用しようとするとき、HP ProtectTools Administrative Console はダイアログ ボックスを開いて、バックグラウンド サービスを開始するかどうかを確認します。**[はい]**をクリックしてバックグラウンド サービスを開始し、システムがブートするたびに自動的に開始するように設定します。

簡易構成

Device Access Manager は、管理者としてデバイスへのアクセスまたはデバイスの参照を実行できる、Device Administrators という新しいユーザー グループをインストール時に作成します。Device Access Manager の簡易構成によってアクセスを制御するデバイスに対して、ユーザーを管理者としてアクセスさせる場合は、そのユーザーをこのグループに所属させてください。

この機能を使用して、以下のクラスのデバイスへのアクセスを拒否できます。

- 管理者以外のユーザーによるすべての USB デバイスへのアクセス
- 管理者以外のユーザーによるすべてのリムーバブル メディア（ディスケット、個人用音楽プレーヤー、USB メモリなど）へのアクセス

- 管理者以外のユーザーによるすべての DVD/CD-ROM ドライブへのアクセス
- 管理者以外のユーザーによるすべてのシリアル ポートおよびパラレル ポートへのアクセス

管理者以外のすべてのユーザーによるデバイス クラスへのアクセスを拒否するには、以下の操作を行います。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 左側のパネルで、[**Device Access Manager**]→[**簡易構成**]の順にクリックします。
3. 右側のパネルで、アクセスを拒否するデバイスのチェック ボックスにチェックを入れます。
4. [**保存**]アイコンをクリックします。

   注記： バックグラウンド サービスが実行されていない場合は、ここで起動が試みられます。[**はい**]をクリックして起動を許可します。

5. [**OK**]をクリックします。

デバイス クラス構成（詳細設定）

特定のユーザーまたはユーザーのグループによるデバイスの種類へのアクセスを許可または拒否することもできます。

ユーザーまたはグループの追加

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 左側のパネルで、[**Device Access Manager**]を展開してから[**デバイス クラス構成**]をクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. [**追加**]をクリックします。[**ユーザーまたはグループの選択**]ダイアログ ボックスが表示されます。
5. [**詳細**]→[**今すぐ検索**]の順にクリックして、追加するユーザーまたはグループを検索します。
6. 使用可能なユーザーおよびグループの一覧に追加するユーザーまたはグループをクリックして[**OK**]をクリックします。
7. [**OK**]をクリックします。

ユーザーまたはグループの削除

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 左側のパネルで、[**Device Access Manager**]を展開してから[**デバイス クラス構成**]をクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. 削除するユーザーまたはグループをクリックして、[**削除**]をクリックします。

ユーザーまたはグループのアクセス拒否または許可

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 左側のパネルで、[**Device Access Manager**]を展開してから[**デバイス クラス構成**]をクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. [**ユーザー/グループ**]で、アクセスを拒否するユーザーまたはグループをクリックします。
5. アクセスを拒否するユーザーまたはグループの横にある[**拒否**]をクリックします。
6. [**保存**]アイコン→[**OK**]の順にクリックします。

ジャスト イン タイム認証（JITA）の設定

管理者は、[ジャスト イン タイム認証の構成]ページでジャスト イン タイム認証（JITA）を使用してデバイスへのアクセスを許可されるユーザーおよびグループの一覧を表示したり変更したりできます。ジャスト イン タイム認証が有効なユーザーは、[デバイス クラス構成]または[簡易構成]ビューで作成されたポリシーで制限されている一部のデバイスにアクセスできます。

シナリオ：[簡易構成]ポリシーは、DVD ドライブや CD-ROM ドライブへのデバイス管理者以外のアクセスをすべて拒否するように構成されています。

結果：ジャスト イン タイム認証が有効なユーザーが DVD ドライブや CD-ROM ドライブにアクセスしようとすると、ジャスト イン タイム認証が有効になっていないユーザーと同じアクセス拒否メッセージが表示されます。また、ユーザーの資格情報を要求する別のポップアップ メッセージが表示されます。ユーザーが Security Manager に正常に認証されると、DVD/CD-ROM ドライブへのアクセスを許可されます。

ジャスト イン タイム認証期間は、設定した時間（分）または 0 分の間有効です。ジャスト イン タイム認証期間を 0 分にすると、認証が有効のままになります。ユーザーは、認証されてからシステムからログオフするまで、デバイスにアクセスできます。

ジャスト イン タイム認証期間は延長も可能です。このシナリオでは、ジャスト イン タイム認証期間が失効する 1 分前に表示されるメッセージをクリックすることにより、再認証しなくてもアクセスを延長できるようにしています。

ユーザーが制限付きまたは無制限のどちらのジャスト イン タイム認証期間を付与されていても、システムからログオフするか、ユーザーを切り替えて他のユーザーとしてログインすると、ジャスト イン タイム認証期間がすぐに期限切れになります。次にユーザーがログインし、ジャスト イン タイム認証が有効なデバイスにアクセスしようとすると、証明情報を要求されます。現時点で、ジャスト イン タイム認証は以下のデバイス クラスに対して使用できます。

- DVD/CD-ROM
- リムーバブル メディア

ここでは、以下のトピックについて説明します。

- ユーザーまたはグループのジャスト イン タイム認証の作成
- ユーザーまたはグループの延長可能なジャスト イン タイム認証の作成
- ユーザーまたはグループのジャスト イン タイム認証の無効化

ユーザーまたはグループのジャスト イン タイム認証の作成

管理者はジャスト イン タイム認証を使用してユーザーまたはグループにデバイスへのアクセスを許可できます。

1. HP ProtectTools 管理者コンソールの左側のパネルで、[**Device Access Manager**]→[**ジャスト イン タイム認証の構成**]の順にクリックします。
2. デバイスのドロップダウン メニューから、[**リムーバブル メディア**]または[**DVD/CD-ROM ドライブ**]を選択します。
3. [**+**]ボタンを使用して、ユーザーまたはグループをジャスト イン タイム認証の構成に追加します。
4. [**有効**]チェック ボックスにチェックを入れます。
5. ジャスト イン タイム認証の期間を必要な時間に設定します。
6. [**適用**]ボタンをクリックします。

これで、選択されたユーザーがログインし、Security Manager に対して認証されて、デバイスにアクセスできるようになります。

ユーザーまたはグループの延長可能なジャスト イン タイム認証の作成

管理者はジャスト イン タイム認証を使用してユーザーまたはグループにデバイスへのアクセスを許可できます。

1. HP ProtectTools 管理者コンソールの左側のパネルで、[**Device Access Manager**]→[**ジャスト イン タイム認証の構成**]の順にクリックします。
2. デバイスのドロップダウン メニューから、[**リムーバブル メディア**]または[**DVD/CD-ROM ドライブ**]を選択します。
3. [**+**]ボタンを使用して、ユーザーまたはグループをジャスト イン タイム認証の構成に追加します。
4. [**有効**]チェック ボックスにチェックを入れます。
5. ジャスト イン タイム認証の期間を必要な時間に設定します。
6. [**延長可能**]チェック ボックスにチェックを入れます。
7. [**適用**]ボタンをクリックします。

これで、選択されたユーザーがログインし、Security Manager に対して認証されて、デバイスにアクセスできるようになります。ジャスト イン タイム認証期間が失効する 1 分前に、ユーザーにジャスト イン タイム認証期間を延長するかどうかを確認するメッセージが表示されます。

ユーザーまたはグループのジャスト イン タイム認証の無効化

管理者は、ジャスト イン タイム認証を使用して、ユーザーまたはグループによるデバイスへのアクセスを無効にできます。

1. HP ProtectTools 管理者コンソールの左側のパネルで、[**Device Access Manager**]→[**ジャスト イン タイム認証の構成**]の順にクリックします。
2. デバイスのドロップダウン メニューから、[**リムーバブル メディア**]または[**DVD/CD-ROM ドライブ**]を選択します。
3. ジャスト イン タイム認証を無効にするユーザーを選択します。
4. [**有効**]チェック ボックスのチェックを外します。
5. [**適用**]ボタンをクリックします。

これで、このユーザーがログインしてデバイスにアクセスしようとしても、アクセスが拒否されるようになります。

詳細設定

[詳細設定]ページには、以下の機能が用意されています。

- デバイス管理者グループの管理
- Device Access Manager によって常にアクセスが許可されるドライブ文字の管理

デバイス管理者グループは、Device Access Manager ポリシーによる制限からデバイス アクセスに関して信頼できるユーザーを除外するために使用されます。この要件に合う可能性の高いユーザーには、システム管理者が含まれます。

管理者は、Device Access Manager がどのユーザーに対してもアクセスを制限しないドライブ文字の一覧を[詳細設定]ビューで設定することもできます。ドライブ文字の一覧を設定するには、Device Access Manager のバックグラウンド サービスが実行されている必要があります。バックグラウンド サービスを開始する最も簡単な方法は、リムーバブル メディアへのデバイス管理者以外のアクセスを拒否するような、簡易構成ポリシーを適用することです。

10 Computrace for HP ProtectTools

Computrace for HP ProtectTools は、お使いのコンピューターをリモートから監視、管理、および追跡できるツールです。

Computrace for HP ProtectTools を有効にすると、Absolute Software Customer Center からツールの設定が行われます。管理者は Customer Center から Computrace for HP ProtectTools を設定し、コンピューターを監視または管理できます。システムの置き忘れや盗難が発生した場合、Customer Center はコンピューターを探索し取り戻すために地域当局に協力します。設定によって、ハードディスク ドライブが消去または交換された場合でも Computrace が動作し続けるようにすることができます。

Computrace for HP ProtectTools を有効にするには、以下の操作を行います。

1. インターネットに接続します。
2. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。
3. Security Manager の左側のパネルで、[**盗難からの回復**]をクリックします。
4. Computrace 有効化ウィザードを起動するには、[**今すぐ有効化**]ボタンをクリックします。
5. 連絡先およびクレジットカードの決済情報を入力するか、あらかじめ購入した製品キーを入力します。

有効化ウィザードが安全に取り引き処理を行い、Absolute Software Customer Center でユーザー アカウントを設定します。完了すると、Customer Center アカウント情報を含む確認用電子メールが送られてきます。

以前に Computrace 有効化ウィザードを実行したことがあり、Customer Center ユーザー アカウントをすでに持っている場合は、HP のサポート窓口に問い合わせて追加ライセンスを購入できます。

Customer Center にログインするには、以下の操作を行います。

1. https://cc.absolute.com/にアクセスします。
2. [**ユーザー名**]フィールドおよび[**パスワード**]フィールドに、確認用電子メールで通知された証明情報を入力して、[**ログイン**]ボタンをクリックします。

Customer Center を使用して、以下のタスクを実行できます。

- コンピューターの監視
- リモートからのデータの保護
- Computrace で保護されているコンピューターの盗難の報告

Computrace for HP ProtectTools について詳しくは、[**詳細情報**]をクリックしてください。

用語集

ATM（Automatic Technology Manager）：
ネットワーク管理者がシステムを BIOS レベルでリモート管理できます。

Drive Encryption キー復元サービス：
SafeBoot の[Recovery Service]。暗号化キーのコピーを保存します。パスワードを忘れたためローカルのバックアップ キーにアクセスできない場合には、このコピーを使用することでコンピューターにアクセスできます。バックアップ キーへのオンライン アクセスを設定するサービスを持つアカウントを作成する必要があります。

Drive Encryption のログオン画面：
Windows が起動する前に表示されるログオン画面。ユーザーは、Windows のユーザー名およびパスワード、またはスマート カードの PIN を入力する必要があります。ほとんどの場合、Drive Encryption のログオン画面で正しい情報を入力すれば、Windows のログオン画面で再度ログインすることなく、直接 Windows にアクセスできます。

Privacy Manager の証明書：
電子メール メッセージおよび Microsoft Office ドキュメントに対する署名や暗号化など、暗号の演算に使用するたびに認証が必要なデジタル証明書。

PSD（Personal Secure Drive）：
機密情報を保護するための記憶領域を提供する機能。

TPM（Trusted Platform Module）内蔵セキュリティ チップ：
HP ProtectTools 内蔵セキュリティ チップの一般的な呼び方。TPM では、ホスト システムに固有の情報（暗号化キー、デジタル署名、パスワードなど）が格納され、ユーザーではなくコンピューターが認証されます。TPM を使用すると、物理的な盗難や外部のハッカーによる攻撃によってコンピューター上の情報が危険にさらされるリスクを最小限に抑えることができます。

TXT：
Trusted Execution Technology。コンピューターのソフトウェアとデータへの攻撃に対するセキュリティ機能を提供するハードウェアおよびファームウェアです。

Windows 管理者：
アクセス権を変更し、他のユーザーを管理するすべての権限を持つユーザー。

Windows ユーザー アカウント：
ネットワークまたは個別のコンピューターへのログオンを承認された個人のプロファイル。

空き領域ブリーチ：
ハードディスク ドライブ上の削除したフォルダーやファイルにランダムなデータを上書きすることによって、削除したフォルダーやファイルの内容が見えないようにし、データの復元がさらに困難になるようにする機能。

暗号化：
権限のない受信者がデータを解読できないように平文を暗号文に変換するための､暗号法で使用されるアルゴリズムなどの手順。データの暗号化にはさまざまな種類があり、ネットワーク セキュリティの基礎として使用されます。一般的な暗号化には、データ暗号化規格（DES）や公開キー暗号があります。

暗号化サービス プロバイダー（CSP）：
明確なインターフェイスを使用して特定の暗号化関数を実行するための暗号化アルゴリズムの提供者またはライブラリ。

暗号化の解除：
暗号化されたデータを平文に変換するための、暗号法で使用される手順。

暗号化ファイル システム（EFS）：
選択されたフォルダー内のすべてのファイルおよびサブフォルダーを暗号化するシステム。

暗号法：
特定の個人だけが解読できるように、データを暗号化および暗号化解除する手法。

[安全に送信]ボタン：
Microsoft Outlook の電子メール メッセージのツールバーに表示されるソフトウェア ボタン。このボタンをクリックすると、Microsoft Outlook の電子メール メッセージに対する署名や暗号化ができます。

移行：
Privacy Manager の証明書および信頼済み連絡先を管理、復元、および転送する作業。

管理者：
「Windows 管理者」を参照してください。

キーの組み合わせ：
特定のキーの組み合わせ。Ctrl ＋ Alt ＋ S キーなどを押すと、自動シュレッドが開始されます。

緊急リカバリ アーカイブ：
他のプラットフォームの所有者キーを使用して基本ユーザー キーを再暗号化できる、保護された記憶領域。

公開：
ユーザーが 1 つ以上のチャット履歴セッションの暗号化を解除して、Contact Screen Name を平文で表示し、セッションを表示できるようにする作業。

公開キー基盤（PKI）
証明情報および暗号化キーを作成、使用、および管理するためのインターフェイスを定義する規格。

資産：
ハードディスク ドライブ上に存在する､個人情報や個人ファイル､履歴データや Web 関連データなどで構成されたデータ コンポーネント。

自動シュレッド：
ユーザーが File Sanitizer for HP ProtectTools で設定したスケジュールに従って実行されるシュレッド。

手動シュレッド：
単一のファイルやフォルダーまたは選択されている複数のファイルやフォルダーに対して、自動シュレッド スケジュールを無視して実行されるシュレッド。

シュレッド：
フォルダーやファイルに含まれるデータの内容をわからなくするアルゴリズムの実行。

シュレッド サイクル：
各ファイルやフォルダーでシュレッド アルゴリズムを実行する回数。選択したシュレッド サイクルの回数が多いほど、コンピューターのセキュリティは高くなります。

シュレッド プロファイル：
あらかじめ指定されている消去方法、およびファイルやフォルダーの一覧。

証明情報：
ユーザーが認証プロセスで特定のタスクに対する適格性を証明するための方法。

[署名と暗号化]ボタン：
Microsoft Office アプリケーションのツールバーに表示されるソフトウェア ボタン。このボタンをクリックすると、Microsoft Office ドキュメントに対する署名、暗号化、または暗号化の解除ができます。

署名欄：
デジタル署名を表示するためのプレースホルダー。ドキュメントに署名すると、署名者の名前と確認方法が表示されます。署名日と署名者のタイトルも表示できます。

シンプル削除：
Windows のファイルやフォルダーの参照情報の削除。空き領域ブリーチを実行しても、ファイルやフォルダーの内容をわからなくするデータをファイルやフォルダーに上書きしないかぎり、その内容はハードディスク ドライブ上に残ります。

信頼済み連絡先：
信頼済み連絡先への招待を承認した人物。

信頼済み連絡先宛てに封印：
電子メールにデジタル署名を付加した上で暗号化し、選択したセキュリティ ログイン方法による認証の後に送信する作業。

信頼済み連絡先の一覧：
信頼済み連絡先を一覧表示したリスト。

信頼済み連絡先の受信者：
信頼済み連絡先になるための招待を受け取った人物。

信頼済み連絡先への招待状：
信頼済み連絡先になることを依頼するために送信された電子メール。

信頼できる IM 通信：
信頼できる送信者から信頼済み連絡先に宛てて、信頼できるメッセージを送信する通信セッション。

信頼できる送信者：
署名および暗号化した電子メールや Microsoft Office ドキュメントを送信する信頼済み連絡先。

信頼できるメッセージ：
信頼できる送信者から信頼済み連絡先に宛てて、信頼できるメッセージを送信する通信セッション。

推奨する署名者：
ドキュメントに署名欄を追加するために Microsoft Word または Microsoft Excel ドキュメントの所有者が指名したユーザー。

スマート カード
コンピューターに挿入するリムーバブル カード。ログオン用の識別情報が保存されています。Drive Encryption のログオン画面でスマート カードを使用してログインするには、スマート カードを挿入し、ユーザー名およびスマート カードの PIN を入力する必要があります。

セキュリティ ログイン方法：
コンピューターへのログインに使用される方法。

デジタル証明書：
デジタル証明書の所有者の身元と、デジタル情報の署名に使用される電子キーのペアとを結びつけることによって、個人または企業の身元を証明する電子的な信用証明書。

デジタル署名：
資料の送信者を証明し、署名された後にファイルが変更されていないことを証明するファイルとともに送信されるデータ。

電源投入時認証：
コンピューターの電源が入ったときにパスワードを要求するセキュリティ機能。

ドメイン：
ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピューターの集合。ドメインには一意の名前が付けられ、各ドメインには一連の共通の規則および手順が設定されます。

ドライブロック（DriveLock）
ハードディスク ドライブをユーザーにリンクして、コンピューターの起動時にユーザーに正しい DriveLock パスワードの入力を要求するセキュリティ機能。

認証：
ユーザーがタスクの実行（コンピューターへのアクセス、特定のプログラムの設定変更、セキュリティ保護されたデータの表示など）を承認されているかどうかを確認するプロセス。

認証機関：
公開キー基盤の運営に必要な証明書を発行するサービス。

ネットワーク アカウント：
ローカル コンピューター上、ワークグループ内、またはドメイン上の Windows ユーザーまたは管理者のアカウント。

廃止パスワード：
ユーザーがデジタル証明書を要求するときに作成されるパスワード。このパスワードは、ユーザーがデジタル証明書を廃止する場合に必要です。これによって、ユーザー自身のみが証明書を廃止できるようになります。

ブリーチ：
「空き領域ブリーチ」を参照してください。

有効化：
Drive Encryption の機能のどれかにアクセスできるようにするために完了する必要のあるタスク。Drive Encryption は、HP ProtectTools Security Manager 管理者コンソール セットアップ ウィザードを使用して有効にします。Drive Encryption を有効化できるのは管理者のみです。有効化処理では、ソフトウェアの有効化、ドライブの暗号化、ユーザー アカウントの作成、およびリムーバブル ストレージ メディア上での初期バックアップ用暗号化キーの作成を行います。

ユーザー：
Drive Encryption に登録された人。管理者以外のユーザーは、Drive Encryption での権限が制限されています。管理者以外のユーザーが実行できる操作は、登録（管理者の許可がある場合）とログインのみです。

リブート：
コンピューターを再起動するプロセス。

索引

P

T

W

あ

い

お

き